Organisation for Economic Co-operation and Development

DAF/COMP/LACF(2020)2

Unclassified

Spanish - Or. English

25 August 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

- Documento de base elaborado por el Secretariado de la OCDE -

28 y 29 de septiembre de 2020

Se hace circular el documento adjunto elaborado por el Secretariado de la OCDE como aportación para el debate en la Sesión I Obtención de pruebas en formato digital en cárteles del Foro Latinoamericano y Del Caribe de Competencia que se llevará a cabo los días 28 y 29 de septiembre, reunión virtual con Zoom.

Las opiniones expresadas en este documento son responsabilidad del autor y no deberán atribuirse al BID, a la OCDE ni sus países miembros respectivos.

Mas documentación sobre este debate están disponible en: oe.cd/laccf.

Por favor, póngase en contacto con la Sra. Cristina Volpin, Cristina.Volpin@oecd.org o por la Sra. Lynn Robertson, Lynn.Robertson@oecd.org si tiene alguna pregunta sobre este documento.

JT03464644

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[*]

RESUMEN

Las empresas recurren cada vez más a la comunicación digital y al almacenamiento digital de los documentos. El cambio que ha traído consigo la digitalización en la forma de operar de las empresas crea tanto oportunidades como una serie de retos para el cumplimiento de la normativa sobre competencia.

Las autoridades de competencia pueden adoptar diversas herramientas y recursos digitales para reforzar su lucha contra los cárteles, que podrían permitirles realizar búsquedas en grandes volúmenes de datos de una manera rápida y con un elevado nivel de precisión. Sin embargo, es posible que la implantación de estas herramientas no siempre resulte sencilla. Pueden plantearse algunos desafíos jurídicos y prácticos relacionados con la protección de la autenticidad de las pruebas incautadas y de los derechos de defensa de la empresa y sus empleados. También pueden requerirse una coordinación interna de los recursos y una cooperación externa para asegurar el pleno aprovechamiento de las oportunidades que ofrecen estas herramientas.

En esta nota temática se analizan algunas de las ventajas y las desventajas de las herramientas digitales más comúnmente utilizadas para la obtención de pruebas y se examinan algunos de los obstáculos jurídicos y prácticos derivados de su utilización, tomando como base casos en los que autoridades de competencia de todo el mundo llevaron a cabo la delicada tarea de recabar pruebas en el marco del cumplimiento de la normativa sobre cárteles.

.

[*] Esta nota temática ha sido elaborada por Harry Hong, Takuya Ohno y Cristina Volpin, de la División de Competencia de la OCDE, y para su redacción se han aprovechado los comentarios de Antonio Capobianco, Lynn Robertson y Sabine Zigelski.

Índice

Boxes

1. Introducción

1. Los cárteles son considerados como la infracción más grave del Derecho de la competencia, y el daño que causan es muy considerable. Se estima que la mediana del sobreprecio de los cárteles en la UE y en algunos países en desarrollo es del 20 %, y solo ligeramente inferior (entre el 16,7 % y el 19 %) en el caso de los Estados Unidos y Canadá (Ivaldi *et al*., 2016, p. 8; Smuda, 2015; Connor, 2014). Entre 1990 y 2016, más de 100.000 empresas se vieron implicadas en prácticas de fijación de precios transfronterizas. Se calcula que los sobreprecios brutos que aplicaron los cárteles durante ese período fueron superiores a 1,5 billones de USD, y que el importe de las ventas afectadas por cárteles internacionales superó en términos nominales los 50 billones de USD (Connor, 2016).

2. La contratación pública también puede ser especialmente proclive a un comportamiento de cártel a través de licitaciones colusorias. El volumen del gasto en contratación pública hace que el impacto negativo de esta situación para los ciudadanos sea especialmente importante. En 2017 la contratación pública representó, en promedio, un 6 % del PIB de la región de América Latina y el Caribe. Sin embargo, una tercera parte de los países de dicha región todavía no han adoptado sistemas de contratación pública electrónicos, que podrían propiciar un aumento de la transparencia y la eficiencia[1]. A pesar de que resulta complicado realizar estimaciones, se considera que la manipulación de las licitaciones ha conllevado un aumento de los costes de entre el 2 % y el 15 %, en función del sector afectado[2].

3. Debido a sus consecuencias, la detección, investigación y enjuiciamiento de conductas de cártel constituye una prioridad de cumplimiento de las normas para muchas autoridades de competencia, tanto de los países de la OCDE como del resto del mundo (OCDE, 2020a, p. 5). En 2018 las autoridades de 49 países adoptaron, en promedio, 10 decisiones relacionadas con cárteles, y 6 en América (OCDE, 2020b, p. 28).

4. Los cambios que ha traído consigo la digitalización han transformado la aplicación de la ley en muchos sectores, incluida la legislación sobre competencia. Las empresas se comunican interna y externamente a través de medios digitales y cada vez crean, almacenan y procesan más información en formato digital. Por consiguiente, las autoridades de competencia deben ajustar sus herramientas de investigación a estos cambios y utilizar cada vez en mayor medida herramientas digitales para la detección y obtención de pruebas de conductas de cártel.

5. Por ejemplo, las herramientas de *screening* o filtrado de datos desempeñan un papel importante en la detección de cárteles. El uso de filtros anticártel ha sido objeto de debate en una mesa redonda dedicada a las investigaciones *ex officio* sobre cárteles y el uso del *screening* para detectarlos, organizada en 2013[3], en una sesión del Foro Latinoamericano y del Caribe de Competencia (FLACC) sobre cómo promover una competencia efectiva en la contratación pública, celebrada en 2016[4] y, más recientemente, en un taller de la OCDE sobre el *screening* de cárteles en la era digital que tuvo lugar en 2018[5].

6. Con frecuencia, las autoridades de competencia utilizan una combinación de *software* avanzado y métodos estadísticos más sencillos y enfoques estructurales y comportamentales para el *screening* de cárteles. Puesto que los filtros se aplican principalmente a las licitaciones colusorias, la digitalización de las empresas privadas y las administraciones públicas y la mayor disponibilidad de datos en formato digital contribuyen a facilitar la detección de ofertas anticompetitivas[6].

7. Existen otras herramientas digitales de apoyo a la obtención de pruebas en formato digital en las labores de cumplimiento de la normativa sobre cárteles. En concreto, las autoridades de competencia cada vez recurren más a técnicas forenses digitales para copiar

y analizar pruebas descubiertas durante las inspecciones y para gestionar de manera eficiente grandes cantidades de datos. Asimismo, estas herramientas han adquirido una mayor importancia a raíz de la pandemia generada por el Covid-19, que, debido a las medidas de distanciamiento social y teletrabajo, ha limitado la capacidad de las autoridades de competencia para realizar inspecciones no anunciadas y entrevistas *in situ* y ha aumentado en mayor medida la importancia de herramientas que permiten analizar pruebas fuera de los locales de las empresas.

8. Si bien las herramientas digitales ofrecen importantes oportunidades para la recogida de pruebas y la investigación, su uso para la aplicación de la normativa sobre cárteles podría plantear algunos desafíos jurídicos y prácticos.

9. Los desafíos jurídicos pueden variar en gran medida dependiendo del régimen jurídico de cada jurisdicción. Sin embargo, se han detectado de manera reiterada tres desafíos jurídicos principales en distintas jurisdicciones con respecto a la obtención de pruebas a través de herramientas digitales. El primero de ellos es la limitación del alcance de la investigación a lo que se considera proporcional, puesto que las herramientas digitales permiten copiar grandes volúmenes de datos a gran velocidad. El segundo desafío, relacionado con este, es el solapamiento entre el acceso a sistemas de almacenamiento de datos y dispositivos electrónicos personales que se encuentren en el lugar de trabajo o contengan información relacionada con el trabajo y el derecho a la privacidad. El tercer reto está relacionado con la ubicación de la información digital y con el hecho de que, si se encuentra fuera de los locales de la empresa, su búsqueda podría trascender el alcance de la orden judicial o la orden de la autoridad de competencia. Dependiendo del marco jurídico aplicable, es posible que, en el caso de que los funcionarios de competencia no los gestionen correctamente, alguno de estos retos jurídicos, o bien todos ellos, den lugar a irregularidades de procedimiento que podrían denunciarse ante los tribunales.

10. También es posible que se planteen desafíos prácticos respecto de la adopción y el uso de herramientas digitales para la obtención de pruebas en procesos judiciales sobre cárteles en relación con la administración de recursos, el desarrollo de la capacidad y la cooperación interna y externa.

11. En primer lugar, las herramientas digitales anteriormente referidas requieren una gran cantidad de recursos en términos de conocimientos especializados, equipos e infraestructura. Esto podría resultar costoso para las autoridades de competencia, que tal vez tengan que elegir la forma más apropiada de adoptar estas herramientas en función de sus limitaciones presupuestarias o de otro tipo (por ejemplo, disponibilidad de soportes informáticos o espacio físico), y también podría requerir una gran cantidad de recursos humanos, ya que podría exigir la contratación de especialistas, la creación de una unidad interna específica o la colaboración con expertos externos (por ejemplo, informáticos y expertos en datos).

12. En segundo lugar, podría ser necesario o útil colaborar con otros órganos nacionales o con otras autoridades de competencia (por ejemplo, en casos de manipulación de las licitaciones o de cárteles transfronterizos) para la obtención de pruebas digitales. Aunque puede que el establecimiento de este tipo de colaboraciones resulte complejo, las autoridades de competencia podrían beneficiarse en gran medida al aprovechar las oportunidades que estas ofrecen.

13. Algunas de estas cuestiones se han abordado, si bien no de manera detallada, en la sesión del FLACC de 2013 sobre las visitas de inspecciones sin previo aviso en investigaciones de conductas anticompetitivas[7] y en la sesión del Foro Global sobre Competencia de 2018 acerca de las facultades de investigación en la práctica, especialmente sobre las inspecciones no anunciadas en la era digital[8]. Además, la

Recomendación del Consejo de 2019 sobre las medidas eficaces contra los cárteles intrínsecamente nocivos se refiere explícitamente a la importancia de que las autoridades de competencia dispongan de facultades efectivas para investigar este tipo de cárteles y, entre otros, para:

> *Acceder a información electrónica que podría contribuir a demostrar la existencia de una violación de las normas sobre cárteles, incluido el material electrónico almacenado en remoto (por ejemplo, en la nube) y tener acceso a técnicas de investigación apropiadas, como la autorización de interceptar y de vigilar las comunicaciones. A tal fin, las autoridades de competencia deberían contar con personal especializado y formado y con equipos de hardware y software apropiados9.*

14. El objetivo de la presente nota temática es analizar los beneficios y los retos a los que se enfrentan las autoridades de competencia al adoptar herramientas específicas para la obtención de pruebas en formato digital en el marco del cumplimiento de la normativa sobre cárteles. En la sección 2 se describen los procesos de obtención, preservación y análisis de pruebas digitales por medio de herramientas forenses informáticas y su funcionamiento. En la sección 3 se abordan los principales desafíos jurídicos asociados a la obtención de pruebas digitales en las investigaciones de cárteles. En la sección 4 se describe la reorganización de los recursos presupuestarios o humanos, incluida la formación digital específica del personal respecto de la adopción de herramientas para la obtención de pruebas digitales. En ella también se analiza la importancia de establecer una colaboración nacional o internacional con el objetivo de recabar pruebas en este ámbito y los retos derivados de esta labor.

2. Métodos para la obtención de pruebas en formato digital en las investigaciones de cárteles

15. Cada vez hay más autoridades de competencia que incluyen datos en formato digital en sus inspecciones con el fin de encontrar pruebas pertinentes. Debido al creciente volumen de datos digitales y a la complejidad que plantean unos entornos informáticos en rápida evolución, obtener pruebas en el curso de una inspección *in situ* se ha convertido en una tarea complicada. Puede que los sistemas informáticos actuales, como la computación en la nube, sean rentables y faciliten a las empresas el almacenamiento de datos y su acceso, pero también pueden crear complicaciones técnicas y jurídicas adicionales para los investigadores y los fiscales a la hora de acceder a los datos electrónicos de una empresa y de recabar pruebas concretas.

16. Por consiguiente, varias autoridades de competencia utilizan herramientas y técnicas digitales avanzadas durante sus investigaciones y sus procedimientos de obtención de datos. Los métodos y los procedimientos adoptados por las autoridades de competencia difieren en función de sus recursos (p. ej., equipos, *software* o personal formado) y del marco jurídico aplicable.

2.1. Obtención de pruebas digitales

17. En las inspecciones no anunciadas, la obtención de datos digitales se realiza principalmente por dos vías. La primera es la incautación física de soportes de datos, como discos duros, CD o memorias USB, que posteriormente se analizarán en busca de las pruebas pertinentes en los locales de la autoridad de competencia.

18. La segunda consiste en examinar los soportes de datos en las instalaciones de la empresa inspeccionada y realizar copias o imágenes forenses[10] de los datos digitales. Para la recogida de pruebas digitales se utilizan herramientas informáticas forenses[11]. Algunas autoridades también utilizan técnicas forenses en tiempo real[12] para capturar datos volátiles a los que no será posible acceder cuando el dispositivo esté apagado (OCDE, 2018a, p. 5).

19. Los equipos de inspección deberían adoptar medidas destinadas a garantizar la integridad de los datos y permitir la autentificación. Para determinar la autenticidad de las pruebas digitales, resulta fundamental mantener una cadena de pruebas y una cadena de custodia[13]. Las actividades relacionadas con la incautación, el examen, el almacenamiento o la transferencia de pruebas digitales deberían documentarse, preservarse y estar disponibles para su examen. Este registro de todos los procesos aplicados a las pruebas digitales debería estar a disposición de una tercera parte independiente para que examine los datos originales siguiendo los mismos pasos y alcance los mismos resultados. En la práctica, por ejemplo, al realizar una réplica de los soportes de datos se utilizan sistemas de bloqueo de escritura para garantizar la integridad de los soportes utilizados como fuente. Además, deberían generarse y guardarse valores de *hash*[14] de todos los datos copiados o replicados que permitan verificar que la copia es idéntica a la información digital original. También es importante documentar todos los pasos de este proceso.

20. Al finalizar la inspección, la información digital no pertinente se devuelve a la empresa o se elimina de forma permanente. En este segundo caso, los inspectores deben limpiar por completo todas las herramientas informáticas forenses en las que se hayan almacenado datos de la empresa (el llamado proceso de «saneamiento»). El objetivo del saneamiento es eliminar por completo los datos de un dispositivo de almacenamiento de tal manera que no sea posible reconstruirlos. Por lo general, los equipos se limpian con instrumentos tradicionales de borrado en un único barrido, de modo que toda la superficie de los discos duros mecánicos se sobrescribirá con un determinado patrón (Comisión Europea, 2015, p. 3; RIC, 2014, p. 21; Van Erps, 2013, p. 214).

21. Una vez realizada la inspección preliminar de los datos digitales recogidos sobre el terreno, algunas autoridades están capacitadas para transportar los datos a sus locales (o a locales policiales o de una autoridad de seguridad equivalente) para seguir buscando pruebas. Esto suele ocurrir cuando los inspectores no logran finalizar la búsqueda y recogida de datos sobre el terreno debido a que el dispositivo se detectó relativamente tarde en el curso de la inspección, a que surgieron problemas técnicos o a que las operaciones durarían demasiado y esto generaría una carga desproporcionada para las actividades cotidianas de la empresa inspeccionada. Este procedimiento se denomina «inspección continuada»[15]. En algunas jurisdicciones, la selección de pruebas digitales podría llevarse a cabo *prima facie* en las instalaciones de la empresa inspeccionada (por ejemplo, mediante la realización de búsquedas empleando palabras clave), y posteriormente se realizarían un examen y una selección en los locales de la autoridad. Algunas autoridades realizan una imagen forense de los soportes de almacenamiento en el lugar de la inspección de manera rutinaria y posteriormente examinan los datos en sus locales, mientras que otras deciden cómo proceder caso por caso (REC, 2013, p. 3; OCDE, 2018a, p. 6; Van Erps, 2013, p. 214). Los posibles retos jurídicos derivados de este procedimiento se analizan en la sección 3.

2.2. Preservación de las pruebas digitales

22. Deben adoptarse medidas para la preservación de las pruebas digitales incautadas durante la inspección. Por «preservación» se entiende impedir el borrado o la destrucción de las pruebas digitales durante su inspección, su transporte o su análisis (véase también el recuadro 2.1).

Recuadro 1. Alteración o destrucción de las pruebas digitales

Aunque el problema de la alteración o destrucción de las pruebas digitales por las partes durante las inspecciones no anunciadas no es específico de las pruebas digitales, este tipo de pruebas pueden transferirse, alterarse o destruirse con mayor facilidad y rapidez que en el caso de las pruebas físicas. Tal y como señaló el ex-Vicepresidente de la Comisión Europea Joaquín Almunia:

> «En la actualidad, la información empresarial se almacena principalmente en entornos informáticos, como los sistemas de correo electrónico, y puede modificarse o borrarse rápidamente. Esta decisión envía un mensaje claro a todas las empresas de que la Comisión no tolerará acciones que puedan socavar la integridad y eficacia de nuestras investigaciones al alterar dicha información durante una inspección».

Si bien es posible que los intentos de ocultar, alterar o destruir pruebas digitales se vean contrarrestados por instrumentos específicos que permitan recuperarlas, pueden obstaculizar considerablemente las labores de la autoridad de competencia y dificultar la búsqueda. Con el fin de disuadir estos intentos, es importante que las autoridades de competencia estén facultadas para imponer sanciones disuasorias considerables y apropiadas.

Por ejemplo, la Autoridad para los Consumidores y los Mercados de los Países Bajos (ACM) impuso en diciembre de 2019 una multa de 1,84 millones de euros a una empresa cuyos empleados habían borrado conversaciones de WhatsApp y habían abandonado grupos de WhatsApp durante una investigación *in situ*. También reafirmó que las empresas investigadas tienen el deber de cooperar, facilitando información precisa y concediendo acceso a los documentos pertinentes, y la obligación de no destruir, ocultar ni eliminar pruebas antes de una investigación no anunciada o en el curso de esta.

En un asunto anterior de 2012, la Comisión Europea multó a dos empresas energéticas checas, Energetický a průmyslový holding a.s. y EP Investment Advisors s.r.o., por no haber bloqueado una cuenta de correo electrónico tal como se les había pedido y haber desviado los correos entrantes. El Tribunal General concluyó que esta forma de actuar constituía una infracción procedimental, aclarando que «*la Comisión tiene la carga de probar el acceso concedido a los datos contenidos en la cuenta de correo bloqueada del Sr. M., pero no le incumbe demostrar que esos datos hayan sido manipulados o suprimidos*».

Fuente: Comisión Europea, comunicado de prensa de 28 de marzo de 2012, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_319.

ACM, comunicado de prensa de 11 de diciembre de 2019, https://www.acm.nl/en/publications/acm-has-imposed-fine-184-million-euros-deleting-whatsapp-chat-conversations-during-dawn-raid.

Tribunal General de la Unión Europea, asunto T-272/12, Energetický a průmyslový holding a.s. y EP Investment Advisors s.r.o. contra Comisión Europea, 26 de noviembre de 2014, EU:T:2014:995, apartado 39.

23. Entre las medidas de preservación se incluyen dejar los dispositivos encendidos durante las técnicas forenses en tiempo real, solicitar que se bloquee el acceso a los buzones de entrada del correo a nivel de servidor, desconectar los cables de red de los ordenadores para evitar un acceso no autorizado, registrar pruebas sobre la atribución del usuario (para identificar al usuario, si posteriormente se cuestionara, y para saber si se han conectado otras personas al ordenador) y proteger los soportes de datos frente a la electricidad estática, los campos magnéticos y los golpes. Además, el procesamiento de las copias de trabajo de los datos digitales es una medida ampliamente aceptada para evitar daños accidentales en los datos digitales originales. Como se ha señalado anteriormente, también resulta esencial mantener una cadena de custodia sólida hasta el archivo del caso (RIC, 2014, p. 22; OCDE, 2018a, p. 6).

2.3. Análisis de las pruebas digitales

24. Tras la fase de obtención de datos, el equipo del caso o los expertos forenses analizan los datos en busca de pruebas. Puesto que las búsquedas digitales pueden generar cantidades enormes de datos, se debe definir algún tipo de estrategia de búsqueda.

25. El método más utilizado es la búsqueda por palabras clave. Las palabras clave se obtienen a partir de una investigación documental, de informantes, solicitantes de clemencia o de las explicaciones recibidas durante la inspección *in situ*. Conforme avanza el análisis, podrán añadirse nuevas palabras clave a la lista. Los *software* específicos de búsqueda forense, como *EnCase* y *Nuix*, pueden detectar versiones mal escritas de las palabras clave y ofrecer resultados más exhaustivos, además de generar resultados basados en algoritmos de autoaprendizaje.

26. Además, estos tipos de *software* forenses permiten la búsqueda por «concepto», que es mucho más avanzada que las búsquedas básicas por palabras clave. La búsqueda por concepto detecta sinónimos y errores de escritura, identifica variaciones de determinadas palabras clave, permite encontrar grupos formados por personas que se comunican regularmente entre sí y localizar comunicaciones en diferentes aplicaciones (p. ej., aplicaciones de mensajería instantánea) y realiza una verificación cruzada automática del contenido de las comunicaciones dentro de los grupos con las palabras clave y sus variaciones. Estas herramientas hacen que para las autoridades resulte mucho más fácil encontrar pruebas pertinentes (Ardiyok y Yüksel, 2016; Van Erps, 2013, p. 214).

27. Otros métodos analíticos confirman la atribución del usuario, visualizan el *spooler* de la impresión, verifican las firmas de los archivos para detectar firmas de archivo incorrectas, buscan información encriptada, investigan los rastros de chats web, webmail, etc. Aplicar más de un método para los datos puede minimizar el riesgo de falsos negativos (RIC, 2014, p. 24; OCDE, 2018a, p. 7).

28. También en este caso es importante documentar todas las medidas adoptadas para extraer las pruebas a fin de mantener la cadena de pruebas y permitir que terceras partes reproduzcan los mismos resultados (OCDE, 2018a, p. 7).

Recuadro 2. Procedimiento para la obtención de pruebas digitales en la Unión Europea

1. Procedimiento de selección sobre el terreno

Hacer una copia forense: los inspectores extraen los archivos posiblemente relevantes del dispositivo investigado (información contenida en determinadas carpetas o determinados tipos de documentos) haciendo una copia forense del contenido. Una vez realizada la copia forense, los inspectores podrían devolver el dispositivo analizado a la empresa investigada.

Cargar, indexar y examinar la copia forense: la copia de toda la información posiblemente relevante se carga en el servidor de la Comisión Europea. A continuación se indexan todos los datos cargados, de modo que toda la información quede catalogada. Una vez indexados, los funcionarios examinan los datos en las unidades de examen.

Etiquetar y copiar: cuando los funcionarios identifican datos pertinentes, proceden a «etiquetarlos». A continuación se copian los datos pertinentes seleccionados en un soporte de datos encriptado (DVD, memoria USB o disco duro), junto con una lista en la que se indiquen el nombre, la ruta y el hipervínculo de cada documento. Se crea una carpeta separada en el soporte de datos en la que se indique el valor de *hash* del contenedor que contenga todos los datos. La lista de documentos debe ir firmada por un representante de la empresa y un funcionario de la Comisión Europea. La empresa recibe una copia del soporte de datos que incluye los datos y la lista.

2. Procedimiento de saneamiento del equipo

Al finalizar la inspección, los funcionarios sanean todo el equipo de la Comisión Europea que se haya utilizado para almacenar información digital de la empresa antes de salir de sus locales.

3. Procedimiento de inspección continuada

La información que se considere posiblemente pertinente basándose en un análisis preliminar o teniendo en cuenta los resultados de búsqueda relacionados con otros datos del mismo depositario se coloca en un soporte de almacenamiento y se encripta. Los funcionarios responsables introducen el soporte de almacenamiento en un sobre precintado y hacen una copia para la empresa.

Posteriormente se traslada el sobre a la Comisión Europea, que se compromete a devolver el sobre precintado a la empresa o a invitarla a asistir a su apertura en las instalaciones de la Comisión Europea y a colaborar en el proceso de inspección continuada. A continuación se identifican los documentos pertinentes como se ha indicado anteriormente («etiquetado», copia en el soporte de datos junto con la lista), la empresa recibe una copia y se procede al saneamiento del soporte.

Fuente: Van Erps (2013).

Recuadro 3. Cuestiones pendientes

1. ¿Cuáles son las herramientas digitales más eficaces para la obtención de pruebas en las investigaciones de cárteles?

2. ¿Cuáles son los mayores beneficios de utilizar herramientas digitales para la obtención de pruebas?

3. ¿Qué dificultades plantea su uso?

4. ¿En qué casos de cárteles han sido más útiles las herramientas digitales para la obtención de pruebas?

3. Retos jurídicos a la hora de obtener pruebas digitales en las investigaciones de cárteles

29. El empleo de herramientas digitales aumenta las probabilidades de que las autoridades de competencia detecten cárteles y recaben información pertinente durante sus investigaciones, puesto que les permiten acceder a una mayor variedad de pruebas e incautarse de un mayor volumen de documentos.

30. Sin embargo, es precisamente esta mayor variedad de posibilidades lo que hace que puedan surgir algunos retos jurídicos a la hora de adoptar estas herramientas debido a las tensiones existentes entre la necesidad de la autoridad de competencia de realizar una investigación detallada y las salvaguardias del debido proceso. Como se ha señalado anteriormente, los retos jurídicos pueden variar en función del régimen jurídico aplicable. Sin embargo, las autoridades de competencia de todo el mundo se enfrentan a una serie de retos comunes relacionados con la obtención de pruebas digitales en casos de cárteles y el ejercicio de sus facultades de investigación. A continuación se analizan algunos de ellos.

3.1. Proporcionalidad de la investigación

31. Por lo general, las inspecciones no anunciadas deben tener un fin específico, lo que significa que, en el momento en que se emita la orden de inspección, la autoridad de competencia debe tener motivos razonables que justifiquen la inspección. El objetivo de la inspección debe ser verificar si una sospecha concreta es fundada o si es posible corroborar determinadas pruebas *prima facie* de una infracción. Las inspecciones no anunciadas no deben ser expediciones meramente especulativas en las que las autoridades de competencia busquen motivos para investigar una infracción. Estos motivos deben ser preexistentes.

32. En muchos países basta con una decisión de las autoridades de competencia para realizar una inspección de los locales de una empresa, pero podría requerirse una orden judicial si las partes deniegan el acceso a los locales (por ejemplo, en el Perú) (OCDE, 2018i, p. 4) o para la inspección de un domicilio privado. En otros países (como Chile)[16] se necesita una orden judicial para inspeccionar los locales de una empresa[17]. Por lo general, las órdenes judiciales o las órdenes de inspección deben incluir información detallada sobre los supuestos hechos que deben verificarse, incluidos el objeto de la investigación, su finalidad y cualquier posible sanción que pueda aplicarse si la empresa no coopera durante la investigación.

33. Una ventaja importante de la digitalización reside en la posibilidad de analizar y copiar rápidamente grandes volúmenes de datos y de información. Si bien la facultad de las autoridades de competencia para hacer copias digitales y recopilar pruebas electrónicas resulta fundamental para llevar a cabo una investigación sobre un trabajo digitalizado, las modalidades empleadas para su ejercicio pueden diferir. Como se indica en la sección 2, algunas autoridades pueden hacer copias digitales de las pruebas para su inspección *in situ*, mientras que otras pueden incautarse de dispositivos o hacer copias para examinarlos en sus oficinas.

34. Por consiguiente, la cuestión que se plantea es si las autoridades de competencia están autorizadas para incautarse de una mayor cantidad de documentos y datos de lo que sería estrictamente pertinente para la investigación, a fin de analizarlos posteriormente en sus locales y hacer copias solo de aquellos que se consideren suficientemente pertinentes como para incluirlos en el expediente.

35. Incluso si, con la ayuda de las herramientas forenses anteriormente descritas, las autoridades de competencia probablemente realicen investigaciones sumamente detalladas, es posible que identificar sobre el terreno los documentos y archivos que es necesario copiar requiera una gran cantidad de tiempo y aumente el riesgo de pasar por alto algunos de ellos. Se deben otorgar a la autoridad de competencia facultades de inspección que le permitan «*cumplir su misión de proteger el mercado [...] de distorsiones de competencia y de sancionar posibles infracciones a las normas sobre competencia en el referido mercado*»[18]. Además, la capacidad para copiar datos con el fin de analizarlos posteriormente también es una forma de reducir al mínimo la intrusión para la empresa y de proteger la integridad de los datos copiados[19].

36. La autoridad mexicana COFECE (OCDE, 2018c), que está facultada para copiar discos duros completos y otras pruebas digitales, pero no puede examinar las pruebas en sus locales, observa lo siguiente:

> *El principal reto al que se enfrenta la Comisión al llevar a cabo inspecciones sorpresivas es que, por ejemplo, no puede incautarse de ordenadores, documentos ni información (solo puede realizar copias de estos). Esto implica que las inspecciones sorpresivas de la Autoridad de Investigación absorben una gran cantidad de los recursos de la Comisión, ya que no puede llevarse simplemente los documentos físicos y dispositivos electrónicos pertinentes para su posterior análisis en la sede de la Comisión. El equipo se ve obligado a copiar los documentos y dispositivos, lo que requiere una cantidad de tiempo y recursos mucho mayor (OCDE, 2018c, p. 7).*

37. En el asunto *Nexans* sometido al Tribunal de Justicia de la Unión Europea, la Abogada General Kokott también alegó lo siguiente:

> *«[p]recisamente a la luz del aumento sustancial del volumen de datos electrónicos generados y almacenados por las empresas [...] parece perfectamente justificado permitir que la Comisión lleve a cabo en sus propios locales el examen de esos datos, que resulta costoso en términos de tiempo, a fin de evitar que el personal de la Comisión quede indebidamente atado a los locales de las empresas inspeccionadas, lo que también podría causar costes elevados».*[20]

38. En la UE, la facultad para «*hacer u obtener copias o extractos, en cualquier formato, de dichos libros o documentación y, cuando lo consideren oportuno, continuar tales búsquedas de información y la selección de copias o extractos en los locales de las autoridades nacionales de competencia o en cualquier otro local que se designe*» se recoge en el artículo 6 (1) c) de la Directiva REC+, que los Estados miembros deberán transponer antes del 4 de febrero de 2021[21].

39. En otras jurisdicciones, la cuestión de si las facultades otorgadas a la autoridad a través de la legislación incluirán la obtención de pruebas digitales, a la que normalmente no se hace referencia en la legislación más antigua, podría depender de la interpretación judicial y de los límites de esta facultad. Sin embargo, puede que esta facultad sea sumamente importante para la realización de investigaciones por parte de las autoridades de competencia y, de haberse previsto las garantías adecuadas, el hecho de que los datos se examinen después de haberse copiado no debería plantear problemas de legitimidad. A este respecto, es especialmente importante que en la orden de inspección se indiquen de manera clara y detallada los motivos de la inspección, el ámbito al que pertenece y las pruebas buscadas, así como que se considere que los documentos y archivos incautados e incorporados en el expediente del caso son, de acuerdo con estos parámetros, pertinentes para la investigación[22].

40. Por consiguiente, el examen de los datos en los locales de la autoridad de competencia podría estar justificado debido a, entre otros motivos: i) el gran volumen de datos que debe analizarse; ii) el hecho de que, en caso contrario, el examen *in situ* llevaría varios días; o iii) la necesidad de posponer el examen de determinados dispositivos (por ejemplo, al no encontrarse presente el dueño del ordenador).

41. Además, cuando las autoridades de competencia decidan recabar pruebas electrónicas, deben poder extraer su «integridad técnica», lo que conlleva, por ejemplo, todo el hilo de una conversación por correo electrónico y sus documentos adjuntos, si bien podrá decidirse que no todos ellos se incluirán en el expediente de investigación[23]. La Comisión Europea ha aclarado este aspecto en su nota explicativa de 2015, en la que afirmó lo siguiente:

> *«cada elemento de prueba seleccionado en el transcurso de la inspección podrá recogerse y consignarse in situ en su totalidad técnica (si, por ejemplo, se selecciona solo un archivo adjunto a un correo electrónico, la exportación final consistirá en dicho correo electrónico junto con todos los archivos adjuntos que pertenezcan a ese mensaje concreto)».*

42. Sin embargo, la incautación de discos duros o servidores enteros para examinar posteriormente los documentos y archivos que contienen puede dar lugar a problemas de privacidad relacionados con el hecho de que los datos podrían incluir información personal, además de la información laboral, o podría trascender el alcance de la investigación definido en la orden de investigación o en la orden judicial. Esta preocupación constituye el meollo de la cuestión de la proporcionalidad de la investigación[24]. Por consiguiente, cuando se le reconoce esta facultad, la autoridad de competencia también debe proteger durante las fases preliminares los derechos de defensa de la empresa, que no deben verse irreparablemente afectados[25].

43. En aquellos casos en que sea necesario examinar los datos en los locales de la autoridad de competencia, con miras a preservar los derechos de defensa de la empresa, y en particular el principio de secreto profesional y la protección de la privacidad, podría ser importante que se respeten determinadas condiciones. Dependiendo del marco jurídico, estas condiciones pueden consistir, por ejemplo, en lo siguiente: i) el precintado del soporte de datos; ii) la eliminación del expediente de todos los datos copiados que no resulten pertinentes[26]; iii) la facilitación de una lista de los documentos copiados; o iv) la presencia de abogados en la apertura del precinto y durante el examen de los datos en los locales de la autoridad de competencia[27].

44. Además de estas medidas de seguridad, o como alternativa a ellas, también es posible incluir algunas garantías integradas en las herramientas digitales empleadas para obtener pruebas, por ejemplo, al garantizar que el *software* o los algoritmos de búsqueda no vayan más allá del alcance de la investigación previsto en la orden de la autoridad o en la orden judicial.

Recuadro 4. Procedimiento seguido por la Comisión Europea en el asunto Nexans France

Mediante decisión de abril de 2014, la Comisión Europea sancionó a una serie de productores europeos, japoneses y surcoreanos de cables eléctricos de alta y muy alta tensión por su participación en un cártel de reparto del mercado.

La Comisión Europea llevó a cabo una inspección en los locales de Nexans France de cuatro días de duración. Durante la inspección, la Comisión Europea realizó copias imágenes del disco duro del ordenador de tres empleados y llevó a cabo una búsqueda con palabras clave basada en la indexación. También precintó la oficina de un cuarto empleado que no se encontraba presente en los locales de la empresa al comienzo de la investigación. Cuando este cuarto empleado regresó al tercer día de la investigación, la Comisión Europea descubrió que se habían eliminado datos de su ordenador. Los funcionarios realizaron copias imágenes del disco duro del ordenador del cuarto trabajador, que introdujeron en sobres precintados y se llevaron consigo a Bruselas.

Posteriormente, la Comisión procedió al examen, siempre en presencia de los abogados de Nexans, abriendo y volviendo a precintar el sobre cada uno de los días que duró el examen. Se imprimieron los documentos pertinentes y se entregó una copia y una lista de dichos documentos a los abogados de la empresa.

La empresa recurrió la decisión. No se alegó una vulneración de los derechos de defensa, puesto que se adoptaron las mismas garantías de procedimiento (como la presencia de los abogados y el precinto de las salas y los sobres) para el examen de los documentos digitales en los locales de Nexans y en los de la Comisión. Sin embargo, Nexans señaló, entre otras cosas, que el artículo 20 (2) del Reglamento 1/2003 no otorga a la Comisión facultad para realizar copias de documentos que no se hayan examinado previamente en los locales de la empresa, ni tampoco para examinar dichos documentos posteriormente en los locales de la Comisión.

Con arreglo a esta disposición, los funcionarios de la Comisión Europea pueden acceder a los locales de las empresas, examinar los libros y la documentación profesional, independientemente de cómo estén almacenados, y hacer copias u obtener extractos.

El Tribunal General concluyó que el artículo 20 (2) del Reglamento 1/2003 no limita la facultad de la Comisión Europea para hacer copias únicamente de los documentos que ya han sido controlados.

La sentencia del Tribunal General se ha recurrido ante el Tribunal de Justicia. Una cuestión similar se encuentra actualmente pendiente de resolución ante el Tribunal de Justicia en el asunto *Prysmian*.

En el caso de los Estados miembros de la UE, esta cuestión se ha abordado mediante la entrada en vigor del artículo 6 (1) c) de la Directiva REC+, que reconoce la facultad de las autoridades de competencia para continuar las inspecciones en los locales de las autoridades nacionales de competencia o en cualquier otro local que se designe, y que los Estados miembros de la UE deberán transponer antes del 4 de febrero de 2021.

Fuentes: Tribunal General de la Unión Europea, T-449/14, Nexans France y Nexans contra Comisión, 12 de julio de 2018, ECLI:EU:T:2018:456; recurso ante el Tribunal de Justicia C-606/18 P; y Tribunal de Justicia de la Unión Europea, C-601/18 P, Prysmian y Prysmian Cavi e Sistemi contra Comisión, pendiente de resolución.

3.2. Acceso a dispositivos electrónicos y datos de carácter personal

45. Una segunda cuestión que podría plantearse en las investigaciones en las que se obtienen pruebas a través de herramientas digitales es la interacción entre las facultades de investigación y el derecho a la privacidad. De manera general, se considera que la protección de la confidencialidad y la privacidad no plantea obstáculos considerablemente diferentes en relación con las pruebas físicas y las digitales (OCDE, 2018d, p. 5). Sin embargo, surge un problema específico en relación con el acceso a los dispositivos y a otros sistemas electrónicos de almacenamiento de datos personales o semipersonales que los empleados podrían tener en los locales de la empresa. Con la expansión de internet y de los teléfonos móviles personales ha aumentado el número de empresas que permiten a sus trabajadores utilizar dispositivos electrónicos personales para fines laborales haya aumentado.

46. Esto significa que, en algunos casos, los dispositivos personales podrían contener pruebas de una infracción o podrían utilizarse vías de comunicación de carácter privado o semiprivado para cometer una violación del Derecho de la competencia.

47. En algunas jurisdicciones, como Francia, la autoridad competente está facultada para inspeccionar dispositivos electrónicos personales que contengan información laboral. En su nota explicativa de 2015, la Comisión Europea indicó expresamente lo siguiente:

> *«Los inspectores podrán inspeccionar el entorno informático (servidores, ordenadores de mesa, ordenadores portátiles, tabletas y otros dispositivos móviles) y todos los soportes de almacenamiento (por ejemplo, CD-ROM, DVD, llaves USB, discos duros externos, cintas de copia de seguridad, servicios en nube) de la empresa. Esto también se aplica a los dispositivos y medios de comunicación privados que se utilizan por motivos profesionales (Trae Tu Propio Dispositivo - BYOD, por las siglas en inglés) cuando se encuentren en los locales»28.*

48. En el Proyecto de Lineamientos de Visitas de Inspección del Perú de 2019 se adopta una postura similar, y también se prevé la posibilidad de que, durante la inspección, los representantes o empleados de la empresa indiquen el carácter personal de los archivos o documentos inspeccionados con el fin de evitar, si así se considera apropiado tras la verificación por parte de los funcionarios, su decomiso[29].

49. Una decisión adoptada por la CNMC de España señala que la empresa investigada no puede denegar el acceso a los archivos, tanto de tipo laboral como personal, así como que dicho acceso, en el caso de que fuera necesario para determinar de manera preliminar la pertinencia de los documentos examinados para la investigación, no constituye una violación de su derecho de defensa[30]. En otras jurisdicciones, como en el caso de Colombia, la jurisprudencia reciente no parece aclarar si la autoridad de competencia también puede ejercer esta facultad para acceder a archivos personales con el fin de realizar un examen preliminar[31].

50. Cuando el marco jurídico no prevé específicamente la posibilidad de que se copien este tipo de datos o la jurisprudencia no aclara esta cuestión, es posible presentar reclamaciones de privacidad ante un tribunal y ralentizar o impedir el ejercicio pleno de la facultad de investigación por parte de la autoridad de competencia.

51. Cuando se detecta una combinación de datos privados y laborales y ni la legislación ni la jurisprudencia facilitan orientaciones específicas al respecto, el enfoque que deberán adoptar las autoridades de competencia también podría depender del método empleado para copiar la información.

52. Si se realiza una copia digital a partir de soportes de datos independientes de los que es posible extraer solo la información pertinente, la empresa investigada podría indicar qué parte de la información es privada para evitar que sea copiada o incautada. En el caso de que surja un desacuerdo sobre la naturaleza de la información, podrían aplicarse procedimientos similares al uso de sobres precintados, es decir, que se incaute la información pero que la autoridad no la examine hasta que se adopte una decisión formal.

53. Si la incautación digital se realiza mediante la obtención de imágenes, la propia naturaleza del proceso hará que no sea posible separar los datos pertinentes de los privados (OCDE, 2013a, p. 13). Una forma de vencer este escollo podría consistir en invitar a los representantes y los abogados de la empresa a los locales de la autoridad de competencia para que asistan al examen de los datos replicados y, antes de proceder al examen, pedirles que indiquen los datos privados que no quieren que se analicen (RIC, 2014, p. 28).

54. Asimismo, la facultad de las autoridades de competencia para examinar dispositivos privados o semiprivados que contengan información laboral también podría adquirir una importancia creciente, en vista de que aplicaciones de mensajería instantánea como WhatsApp, Skype o MSN se encuentran cada vez con mayor frecuencia entre las vías de comunicación preferidas utilizadas para alcanzar y mantener un acuerdo anticompetitivo[32].

55. Además del uso cada vez más ambiguo que se hace de medios de comunicación y almacenamiento de datos para fines empresariales y personales generado por la revolución de internet, la pandemia de Covid-19 y las políticas de teletrabajo adoptadas por empresas de todo el mundo han acentuado la difuminación de la frontera entre los dispositivos empresariales y los personales. En esta nueva realidad, es posible que la facultad de las autoridades de competencia para buscar e incautarse de información de carácter laboral almacenada en dispositivos personales sea cada vez más crucial.

56. Cuando se presenten reclamaciones relacionadas con la privacidad de los datos, es importante que se evalúen con rapidez y detalle para determinar su validez, con miras a evitar el riesgo de que se lleven a cabo comunicaciones ilícitas a través de dispositivos personales exclusivamente con el fin de evitar la aplicación de la ley y que esto obstaculice y prolongue la investigación. Mientras que en algunas jurisdicciones la investigación la llevará a cabo un funcionario que trabaje en el caso, en otras lo hará una tercera parte independiente, como por ejemplo personal de la autoridad de competencia no implicado en el caso o una autoridad judicial (RIC, 2014, p. 28).

Recuadro 5. Retraso de la investigación debido a obstáculos relacionados con cuestiones de procedimiento: el caso de los bancos portugueses

En 2019, la autoridad de competencia de Portugal (AdC) multó a 14 bancos por haber intercambiado información comercial sensible durante más de 10 años. La cuantía total de la multa impuesta a los bancos implicados en esta práctica fue de 225 millones de euros.

La investigación se inició con una solicitud de clemencia y consistió en la realización de inspecciones sorpresivas en 25 lugares. En el curso de la investigación, algunos de los bancos investigados presentaron recursos de procedimiento relacionados con, entre otras cosas, la confidencialidad de la información incautada. Los bancos investigados presentaron 26 recursos sobre cuestiones de procedimiento que dieron lugar a 43 procesos judiciales. Aunque solo 5 de las decisiones judiciales adoptadas fueron favorables para el banco investigado, los procesos judiciales hicieron que la investigación se pausara durante más de 360 días.

Si bien este caso estaba relacionado con la confidencialidad de la información incautada, muestra el impacto que pueden tener los recursos (fundados o infundados) por motivos de procedimiento en la duración de la investigación.

Fuente: Parr, «Portuguese decision shows banks filed 26 court proceedings during probe», 10 de enero de 2020, https://app.parr-global.com/intelligence/view/1926305.

3.3. Acceso a servidores situados fuera de los locales de la empresa

57. Un tercer problema que se plantea está relacionado con la ubicación de la información digital, puesto que el lugar de almacenamiento de esta, por ejemplo, en servidores o en la nube, no suele corresponder a la misma ubicación física que el punto de entrada de los datos. Por consiguiente, puede que las inspecciones requieran acceder a datos almacenados en servidores o en otros sistemas de almacenamiento situados en otros emplazamientos físicos (por ejemplo, en otra dirección de la empresa investigada o en los locales de un tercero, tanto en la misma jurisdicción como en otra) o bien en línea, es decir, sin ubicación física (RIC, 2014, p. 29).

58. Con respecto a esta cuestión, la Red Internacional de Competencia (RIC) identifica dos tipos de enfoques. El primero de ellos, denominado «enfoque basado en el acceso», consiste en que la autoridad de competencia puede buscar e incautarse de cualquier dato que pueda consultarse, utilizarse o controlarse desde los locales de la empresa. La ubicación del lugar de almacenamiento carece de pertinencia. Como se ha indicado en la introducción, la Recomendación del Consejo de la OCDE de 2019 sobre las medidas eficaces contra los cárteles intrínsecamente nocivos favorece este enfoque al referirse a la facultad de las autoridades de competencia para acceder a información electrónica que podría contribuir a demostrar la existencia de una violación de las normas sobre cárteles, incluido el material electrónico almacenado en remoto (p. ej., en la nube)[33].

59. El segundo enfoque, denominado «enfoque basado en la ubicación», prevé que, cuando los datos no estén almacenados en los locales de la empresa, y habida cuenta de que una orden de inspección solo permite entrar en los locales de la persona jurídica a la que se refiere, la ubicación alternativa también debe figurar en la orden de la autoridad o del juez (RIC, 2014, pp. 28 y 29).

60. En este segundo caso, podría ser mucho más complicado para la autoridad de competencia acceder a las pruebas pertinentes. En primer lugar, tendrá que averiguar el lugar exacto en que se encuentran los servidores dentro de otra empresa. Esto no será posible en el caso de los sistemas de computación en nube a través de los que se almacenan datos en línea. En segundo lugar, la empresa podría aprovechar el tiempo que se requiere para acceder a la ubicación alternativa, si se descubriera una vez iniciada la investigación, para transferir, destruir o alterar las pruebas (véase el recuadro 2.1).

61. En algunas jurisdicciones, la legislación reconoce el enfoque basado en el acceso. Por ejemplo, en el artículo 6 (1) b) de la ya mencionada Directiva REC+ se prevé la facultad para «*examinar los libros y cualquier otra documentación en relación con la actividad empresarial, independientemente del soporte en que se almacene, y tener derecho a acceder a toda información a la que tenga acceso la entidad inspeccionada*». En otras jurisdicciones, puede que el uso del enfoque basado en el acceso todavía resulte controvertido[34].

62. En aquellos casos en que la autoridad de competencia no aplique el «enfoque basado en el acceso », que resulta más favorable, también podría ser necesario adoptar otras formas de cooperación similares a la Red 24/7 para Delitos de Alta de Tecnología del G8, que ofrece puntos de contacto en los países integrantes para solicitar apoyo inmediato en el marco de una investigación que implique pruebas electrónicas, lo que incluye solicitudes de preservación de datos[35] o cooperación con organismos fuera de la jurisdicción pertinente. La RIC señaló que, en estos casos, las autoridades de competencia recurren a la posibilidad que ofrecen los tratados o los acuerdos de asistencia jurídica mutua para recabar información digital (RIC, 2014, p. 29).

63. Sin embargo, es importante subrayar que las empresas pueden seleccionar estratégicamente como «centro» de un cártel transfronterizo una jurisdicción en la que sea más complicado para una autoridad de competencia acceder rápidamente a las pruebas en el marco de una investigación, buscando de tal modo un «foro de conveniencia» en cuanto a las garantías de procedimiento y unas facultades de investigación más débiles (Scordamaglia-Tousis, 2014, p. 196). Esto hace que la convergencia de las facultades de investigación y el debido proceso en todos los países sea sumamente importante.

Recuadro 6. Cuestiones pendientes

1. ¿Cuáles son las mejores vías para garantizar que el procedimiento de inspección continuada se lleve a cabo respetando plenamente el debido proceso?
2. En un mundo en que el teletrabajo se ha generalizado debido a las medidas de distanciamiento por Covid-19, ¿debería estar permitido registrar los dispositivos electrónicos personales en cualquier momento? ¿Cómo puede encontrar una autoridad de competencia el equilibrio necesario entre garantizar un análisis detallado de las pruebas pertinentes y proteger la privacidad?
3. ¿Cómo garantizan las autoridades de competencia que se respeten los derechos de defensa de las empresas al recabar pruebas digitales en las investigaciones de cárteles?
4. ¿Qué estrategias han adoptado las autoridades de competencia para superar las dificultades encontradas al acceder a servidores o a información almacenados en sistemas digitales en la nube? ¿Cuáles son las mejores vías para impedir la destrucción o alteración de pruebas cuando este proceso requiere mucho tiempo?
5. ¿Puede utilizarse la cooperación internacional para estimular la convergencia de las facultades de investigación y el debido proceso en todos los países?

4. Desarrollo de la capacidad para recabar pruebas digitales en las investigaciones de cárteles

64. La obtención de pruebas digitales requiere una inversión considerable para lograr unos conocimientos (p. ej., técnicas forenses digitales, análisis de datos e inteligencia artificial), unas herramientas (p. ej., equipos y *software*) y una infraestructura (p. ej., salas para el análisis forense) específicos que deben actualizarse con frecuencia en función de la rápida evolución de la tecnología. Desarrollar y mantener la capacidad para recabar pruebas digitales es más costoso que en el caso de la capacidad para obtener pruebas tradicionales, y requiere el apoyo y la comprensión del personal directivo.

65. Asimismo, muchas autoridades de competencia se enfrentan a congelaciones o limitaciones presupuestarias. De hecho, tal y como se pone de relieve en las *OECD Competition Trends 2020* (Tendencias de la OCDE en materia de competencia de 2020), el presupuesto medio de las autoridades de competencia se redujo aproximadamente un 5 % en términos reales entre 2015 y 2018 (OCDE, 2020b, p. 11). En vista de la presión para los presupuestos públicos generada por el brote de Covid-19, parece poco probable que esta tendencia se revierta en un futuro cercano.

66. Por lo tanto, será incluso más importante para las autoridades de competencia seguir utilizando de manera eficiente sus limitados recursos al diseñar su estructura interna para la obtención de pruebas digitales. Además, la cooperación externa con otros organismos debería ayudar a lograr una utilización más eficiente de los recursos a la hora de organizar la recogida de pruebas digitales.

4.1. Organización interna para la obtención de pruebas digitales

67. Algunas autoridades de competencia han invertido una cantidad importante de recursos para desarrollar su capacidad de obtención de pruebas digitales. Por ejemplo, la autoridad de competencia de Brasil (CADE) empezó a desarrollar herramientas de minería de datos y filtros económicos en 2014 para prestar apoyo al personal encargado de las investigaciones y los gestores de casos (véase el proyecto «Cérebro» en el recuadro 4.1). La autoridad de competencia de México (COFECE) también ha invertido recursos en la formación de expertos forenses e investigadores, así como en *hardware* y *software* (OCDE, 2018c, p. 7). Aunque no cabe duda de que estas medidas de desarrollo de la capacidad resultan fructíferas, garantizar un presupuesto que cubra los elevados costes derivados de dichas medidas podría ser un desafío considerable para las autoridades de competencia. En este sentido, la RIC recomienda disponer de un presupuesto anual o plurianual específico para la obtención de pruebas digitales (RIC, 2014, p. 14).

68. El presupuesto, que en última instancia determina los recursos de que disponen las autoridades, influirá en el modo en que se organiza la capacidad de obtención de pruebas dentro de la autoridad. Algunas autoridades de competencia cuentan con una unidad informática forense permanente para la obtención de pruebas (p. ej., en la UE (OCDE, 2018d, p. 4), Portugal (OCDE, 2018e, p. 15) o Corea (OCDE, 2018f, p. 5)). Se ha informado de que estas unidades, compuestas por expertos en técnicas forenses digitales que trabajan en estrecha colaboración con funcionarios y expertos informáticos internos de los organismos para la obtención de pruebas digitales (y posiblemente para el análisis de datos en mayor escala), han aportado un considerable valor añadido a la obtención de pruebas digitales[36].

69. Dependiendo de las circunstancias del caso, varias autoridades han recurrido a expertos informáticos forenses externos que colaboraron estrechamente con el personal y los expertos informáticos internos de la autoridad (p. ej., en Sudáfrica (OCDE, 2018g, p. 2) o en Australia (OCDE, 2018h, p. 3)). Como ha señalado la RIC, esta externalización podría requerir un acuerdo de confidencialidad como garantía en relación con la información confidencial que se pone a disposición de los expertos informáticos forenses externos (RIC, 2014, p. 14). Otro reto parece ser el de integrar correctamente a los expertos externos en el equipo de investigación para maximizar los beneficios de contar con especialistas en informática en el equipo. En función del servicio prestado, puede que los expertos externos resulten sumamente costosos. En este sentido, la RIC recomienda mantener una capacidad informática interna mínima, incluso cuando se recurra a la externalización, con el fin de garantizar que se preste un servicio apropiado a un precio razonable (RIC, 2014, p. 14). Unos conocimientos informáticos mínimos por parte del personal de las autoridades y unos conocimientos mínimos sobre el Derecho de la competencia por parte de los expertos informáticos externos también facilitarían una integración fluida de los diferentes expertos en el equipo de investigación.

70. Independientemente de cómo esté organizada la capacidad de obtención de pruebas digitales interna, resulta indispensable garantizar que quienes se encargan de recabar este tipo de pruebas estén correctamente formados para ello. Esto podría lograrse mediante el desarrollo de las competencias del personal existente o la contratación de expertos externos. Las competencias necesarias para la obtención de pruebas digitales engloban diferentes ámbitos de especialización. Por ejemplo, incluyen las técnicas forenses digitales, es decir, la aplicación de técnicas científicas para identificar, preservar, recuperar y analizar la información digital y presentar hechos y opiniones al respecto (OCDE, 2018a, p. 4). Otras tecnologías emergentes, como la inteligencia artificial, el internet de las cosas, los macrodatos y la cadena de bloques, también serían útiles para la detección de casos que

requieren un conocimiento técnico y económico detallado del comportamiento de las empresas en lo relativo a los datos y los algoritmos (véase el recuadro 4.1). Como puso de relieve acertadamente la Autoridad de Competencia y Mercados del Reino Unido, los organismos encargados de la aplicación de la ley también pueden aprovechar el poder de los algoritmos para examinar grandes conjuntos de datos a fin de evaluar las repercusiones en términos de competencia (OCDE, 2017, p. 12). Además, es posible que quienes se ocupen de la obtención de pruebas digitales deban recibir formación sobre las normas jurídicas pertinentes y sobre los retos anteriormente descritos para garantizar que el procedimiento se lleve a cabo respetando los límites del marco jurídico aplicable.

Recuadro 7. Screening de cárteles: una herramienta de detección proactiva de cárteles

Las herramientas de *screening* o filtrado de cárteles se han convertido en importantes instrumentos proactivos para reducir la dependencia de herramientas reactivas, como la denuncia de irregularidades o las solicitudes de clemencia. La creciente disponibilidad de datos y capacidad informática ofrece a las autoridades de competencia vías eficaces para detectar señales atípicas o comportamientos sospechosos asociados a la colusión.

El *screening* o filtrado de cárteles es sin duda una herramienta eficaz para detectar los cárteles, pero también genera un efecto disuasorio adicional al animar a las empresas a presentar solicitudes de clemencia, firmar acuerdos de cese y desistimiento y denunciar conductas anticompetitivas ante las autoridades de competencia.

El *screening* es una metodología de detección diseñada para ayudar a las autoridades de competencia a determinar qué mercados o sectores son más proclives a las actividades de cártel, y en algunos casos también puede señalar conductas potencialmente cartelísticas que merezcan una especial atención (OCDE, 2013, p. 5). Esto significa que, cuando a través de un filtro se selecciona un sector, esto no garantiza el enjuiciamiento, sino una investigación más exhaustiva que opone directamente la colusión y la competencia como explicaciones contrapuestas del comportamiento de mercado. Por lo tanto, el *screening* es la primera fase de un proceso de múltiples etapas que puede culminar o no con un proceso judicial (Harrington, 2007, p. 2)

Cada vez se publica más bibliografía sobre la detección de cárteles, que puede dividirse de manera general en dos vertientes (Imhof, Karagök y Rutz, 2018, p. 237; OCDE, 2013, p. 5). El primer enfoque, comúnmente denominado *screening* «estructural», se basa en lo que las teorías económicas e investigaciones empíricas nos dicen sobre la relación entre las características de los mercados y la probabilidad de que estos sufran colusión, básicamente identificando ciertas características estructurales de productos o mercados que la facilitan. Este enfoque podría permitir a una autoridad de competencia supervisar numerosos mercados o sectores para identificar aquellos en los que cabe esperar la aparición de cárteles.

El segundo enfoque, basado en el *screening* «conductual», se emplea para indicar si un mercado específico ha sido víctima de la colusión. Obviamente, no es fácil observar pruebas inequívocas de cartelización, y destaparlas reviste gran dificultad. Sin embargo, la teoría económica y el análisis de los datos observados en cárteles han identificado diferentes tipos de huellas que pueden dejar a su paso la creación, existencia y disolución de un cártel. Los filtros conductuales están diseñados para detectar esas huellas.

Estos dos enfoques no son incompatibles. Al contrario, suelen considerarse complementarios, de tal manera que, si el *screening* estructural da resultados positivos, las autoridades pueden proceder a una revisión más precisa basada en el comportamiento de las empresas y su coherencia con el proceso competitivo.

El *screening* es un método que requiere una gran cantidad de recursos y datos. En todas las etapas de la aplicación de los filtros es necesario disponer de información y datos suficientes, pertinentes y exactos: desde la creación del filtro hasta su aplicación e interpretación de los resultados. Tener acceso a esta información es una cuestión clave en cualquier metodología empírica. Asimismo, los filtros pueden ser muy sensibles a la cantidad y calidad de los datos de que disponen. Por ejemplo, aplicar un filtro de desviación de precios a datos agregados (p. ej., precios medios anuales o mensuales) obtenidos en estudios de mercado podría arrojar resultados completamente distintos que si se empleara el mismo filtro a datos desagregados (p. ej., cotizaciones diarias).

Algunas autoridades de competencia han utilizado métodos de *screening* de cárteles de forma generalizada, entre los que se incluyen los siguientes.

Proyecto «Cérebro» de Brasil

El Consejo Administrativo de Defensa Económica (CADE) ha llevado a cabo desde 2014 un proyecto de *screening* llamado «Cérebro» (cerebro). Cérebro es una plataforma que permite integrar grandes bases de datos sobre contratación pública mediante la aplicación de herramientas de minería de datos y filtros económicos capaces de identificar y medir la probabilidad de que se formen cárteles en licitaciones públicas.

Las herramientas de minería de datos de Cérebro permiten automatizar los análisis previamente realizados por los investigadores y los gestores de casos. El objetivo es detectar pruebas de cárteles en el marco de licitaciones públicas, como hechos o patrones de conducta sospechosos o inverosímiles, y facilitar información pertinente para la investigación de los casos. Los filtros económicos de la plataforma se basan en bibliografía y econometría especializadas. Su objetivo es facilitar pruebas generalizadas de la existencia de cárteles basadas en datos relacionados con los precios, los costes, los márgenes de beneficio, la cuota de mercado, etc. Mediante la identificación del comportamiento de las empresas descrito en los artículos académicos, el CADE elaboró modelos matemáticos en forma de pruebas estadísticas para su uso general en una especie de proceso de ingeniería inversa.

El empleo de la herramienta Cérebro ha dado lugar a la puesta en marcha de algunas investigaciones. Todavía se encuentra en una fase temprana, y los tribunales están analizando si la información que facilita es suficiente para alcanzar el mínimo necesario para que se emita una orden para una inspección sorpresiva.

Programa ALCO de Colombia

La autoridad de competencia de Colombia (SIC) ha participado desde 2013 en un proyecto destinado al desarrollo de un *software* para el rastreo de datos sobre contratación pública (ALCO). El objetivo del programa es ayudar a identificar patrones de conducta de los licitadores que sugieran un comportamiento colusorio y notificárselo a la SIC.

Chile

La autoridad de competencia de Chile (FNE) utiliza datos sobre contratación pública para llevar a cabo ejercicios de *screening*. La FNE y el organismo central para la contratación pública, ChileCompra, tienen un acuerdo de cooperación que permite a la

FNE realizar un seguimiento de las licitaciones a través de la base de datos de ChileCompra.

México

En 2015, la autoridad de competencia de México (COFECE) creó una unidad de inteligencia de mercado como parte de su Autoridad de Investigación dedicada íntegramente al seguimiento de los mercados y al filtrado de datos de mercado para recopilar pruebas suficientes que permitan iniciar investigaciones antimonopolio. Entre 2016 y 2019, aproximadamente el 20 % de las investigaciones se iniciaron gracias a los hallazgos de dicha unidad de inteligencia de mercado.

Perú

La autoridad de competencia del Perú (INDECOPI) estableció entre 2007 y 2013 indicadores para detectar prácticas de manipulación de las licitaciones en la adquisición pública de carburante líquido. Estos indicadores se basan en criterios económicos y datos facilitados por el Organismo Supervisor de las Contrataciones del Estado del Perú (OSCE).

Sistema de Análisis de los Indicadores de Colusión en Licitaciones (BRIAS) de Corea

En 2006, la Comisión de Comercio Justo de Corea creó el Sistema de Análisis de Indicadores de Colusión en Licitaciones (BRIAS) para ayudar a detectar la manipulación de las licitaciones. El BRIAS es un sistema informático de análisis cuantitativo automático que analiza grandes cantidades de datos sobre la contratación pública en línea y, en función de los indicadores que lleva incorporados, cuantifica la probabilidad de que se manipulen las licitaciones.

El BRIAS recopila la información sobre la contratación pública en línea relativa a grandes contratos adjudicados por administraciones centrales y locales en un plazo de 30 días a partir de su adjudicación. Posteriormente, el sistema analiza los datos y genera una puntuación sobre la probabilidad de que se produzca manipulación evaluando factores como el método de licitación, el número de licitadores, el número de ofertas conformes, el número de ofertas no conformes, los precios de licitación por encima del precio estimado y el precio del licitador ganador. Cada uno de estos factores tiene asignado un valor ponderado, y en última instancia se sumarán todos ellos. Por ejemplo, una mayor tasa de ofertas conformes y un menor número de empresas participantes son indicativos de una posible colusión. Además, todas las ofertas se filtran según criterios de búsqueda como el nombre del candidato ganador o las ofertas con una puntuación similar.

En el BRIAS participaban un total de 16 organismos de contratación pública, incluidos organismos administrativos centrales y empresas de propiedad estatal. Entre 2015 y 2019, el BRIAS seleccionó más de 5.600 casos para su posterior análisis, y la Comisión de Comercio Justo de Corea inició 783 investigaciones.

Fuente: OCDE (2020; 2019; 2016); Comisión de Comercio Justo de Corea.

4.2. Cooperación externa para la obtención de pruebas digitales

71. Además de la organización interna eficiente, la cooperación externa debería ayudar a reforzar la capacidad de obtención de pruebas digitales de las autoridades de competencia. Esta cooperación puede adoptar numerosas formas, como acuerdos de cooperación bilaterales o multilaterales, memorandos de entendimiento, tratados de asistencia jurídica mutua o colaboración *ad hoc*[37]. Podría establecerse con otros organismos nacionales (por ejemplo, reguladores financieros o de telecomunicaciones), así como con otras autoridades de competencia.

4.2.1. Cooperación con otros organismos nacionales

72. La obtención de pruebas digitales no solo está diseñada para su uso en investigaciones sobre competencia, sino también para la detección de otras conductas ilegales, como la manipulación de los precios e índices bursátiles y de los bienes, la gestión de los ingresos, las opciones de compra de acciones con carácter retroactivo, las operaciones basadas en información privilegiada y la evasión fiscal. Muchos organismos públicos, como las autoridades de regulación financiera, los organismos de contratación y los reguladores de la energía y las telecomunicaciones, también utilizan herramientas digitales al desempeñar sus responsabilidades en materia de control y aplicación de la ley. Por consiguiente, colaborar con estos organismos ofrece un importante potencial para la creación de sinergias en lo relativo a la obtención de pruebas digitales.

73. En este contexto, varias autoridades de competencia han establecido un marco de cooperación con otros organismos públicos para la recuperación, el copiado y el análisis de pruebas digitales. Por ejemplo, la autoridad de competencia de Chile (FNE) concertó un acuerdo de cooperación con la Dirección de Compras y Contratación Pública del Gobierno (Chilecompra) que permite a la FNE realizar un seguimiento de las licitaciones a través de la base de datos disponible entre los recursos tecnológicos de Chilecompra (OCDE, 2013, p. 99; para otros ejemplos, véase el recuadro 4.1). La cooperación también podría consistir en la organización de seminarios, formaciones o talleres conjuntos y en el intercambio de conocimientos y experiencia en materia de obtención de pruebas digitales. Por ejemplo, la Dirección General de Política de Competencia, Asuntos de los Consumidores y Control del Fraude de Francia (DGCCRF), que ha desarrollado conocimientos especializados en el ámbito de las inspecciones digitales desde principios del año 2000, compartió sus conocimientos con la autoridad de competencia de Francia creada en 2008 (CE, 2016, p. 6). Este tipo de cooperación parece relativamente más fácil de establecer y, por lo tanto, debería fomentarse, puesto que no requiere acuerdos ni memorandos de entendimiento oficiales.

Recuadro 8. Recomendación de la RIC sobre la cooperación con otros organismos públicos

En cuanto a la cooperación con otros organismos públicos para la obtención de pruebas en formato digital, la RIC recomienda que se describan el alcance y la naturaleza de dicha cooperación en un protocolo que abarque las responsabilidades y los procedimientos de los organismos colaboradores durante el proceso de obtención de pruebas digitales.

Según la RIC, el protocolo debería abarcar las responsabilidades y los procedimientos de los organismos colaboradores durante el proceso de obtención de pruebas digitales. Además, debería detallar cómo se gestionarán e intercambiarán los datos extraídos.

La RIC también señala elementos concretos que sería útil plasmar en dicho protocolo de cooperación:

- las horas que aportará el otro organismo y cómo se calcularán (horas extraordinarias en una misión, períodos concretos, etc.), el tiempo máximo en misión, la formación para el equipo;
- el material que se facilitará: *hardware*, *software*, material de apoyo;
- los nombres o cargos del personal que prestará el apoyo;
- la antelación mínima con la que se informará al personal de apoyo antes de una intervención;
- el precio del servicio o contrato; y
- la duración del contrato y las modalidades de examen.

Fuente: RIC, 2014, p. 14.

4.2.2. Cooperación con otras autoridades de competencia

74. La cooperación internacional debería ayudar a desarrollar de manera eficiente una capacidad de obtención de pruebas digitales. Dicha cooperación podría darse, por ejemplo, en forma de actividades conjuntas de desarrollo de la capacidad. De hecho, varias autoridades de competencia han establecido un programa de cooperación para fomentar su capacidad de obtención de pruebas digitales. Por ejemplo, en el marco de la Red Europea de Competencia (REC), en 2010 se creó un grupo de trabajo sobre informática forense destinado a servir como foro para el intercambio de información y mejores prácticas sobre cuestiones técnicas y jurídicas relativas al uso de herramientas informáticas forenses[38]. En vista del desarrollo y la importancia de la inteligencia artificial en las investigaciones de cárteles, se ha modificado recientemente el nombre del Grupo de Trabajo sobre Informática Forense del REC, que ha pasado a llamarse Grupo de Trabajo sobre las Investigaciones Digitales y la Inteligencia Artificial[39].

75. La cooperación internacional también podría ampliarse a aspectos más sustantivos de la obtención de pruebas digitales. Esto resulta especialmente pertinente en lo relativo al acceso a pruebas digitales ubicadas en el extranjero y al intercambio de pruebas digitales entre autoridades (dentro de los límites del marco jurídico pertinente). Sin embargo, tal como se ha puesto de relieve en el trabajo previo de la OCDE, a pesar de que la cooperación internacional en casos de cártel ha alcanzado niveles históricos en los últimos años, parece que siguen existiendo una serie de obstáculos que impiden una cooperación eficaz. Entre ellos cabe mencionar la incapacidad para intercambiar información confidencial, las dificultades para obtener pruebas situadas fuera de la jurisdicción pertinente y la realización de inspecciones digitales conjuntas.

Recuadro 9. Cuestiones pendientes

- ¿Cómo pueden garantizar las autoridades de competencia un presupuesto suficiente para desarrollar la capacidad de obtención de pruebas digitales?

- ¿Cómo pueden crear las autoridades de competencia su capacidad de obtención de pruebas digitales interna? ¿Deberían centrarse en desarrollar las competencias del personal existente o contratar a expertos externos?

- ¿Cuáles son las mejores prácticas para una mejor integración de los expertos informáticos forenses externos en el equipo de investigación?

- ¿Cuáles son las competencias clave que deben poseer los funcionarios y los expertos forenses para la obtención de pruebas digitales? En este sentido, ¿cuál sería el perfil ideal del personal dedicado a esta labor? ¿Sería más apropiado contar con expertos en competencia con conocimientos forenses o con expertos forenses con formación en Derecho de la competencia?

- ¿Cómo pueden garantizar las autoridades de competencia que la cooperación con otros entes reguladores públicos y otras autoridades de competencia para obtener pruebas digitales sea eficaz? ¿Qué tipo de cooperación convendría establecer?

- ¿Cuáles son los obstáculos a la cooperación internacional para la obtención de pruebas digitales? ¿Qué medidas podrían adoptarse para hacerles frente?

5. Conclusiones

76. En el presente documento temático se resumen algunos de los desafíos jurídicos y prácticos a los que podrían enfrentarse las autoridades de competencia con respecto a la obtención de pruebas digitales en las investigaciones de cárteles. Cada vez se crean más herramientas para la obtención de pruebas digitales que se encuentran en continua evolución, lo que amplía las facultades de las autoridades de competencia para recabar grandes volúmenes de datos y de información de una manera rápida.

77. Asimismo, es probable que estas herramientas cobren una mayor importancia en el marco de la actual pandemia de Covid-19, que, debido a las medidas de confinamiento y las políticas de teletrabajo adoptadas por muchas empresas, ha cambiado la forma de operar de las autoridades de competencia y de las empresas.

78. Sin embargo, las nuevas oportunidades pueden, por una parte, plantear una serie de retos jurídicos relacionados con su alcance, que podría chocar con el derecho de defensa de la empresa o con el derecho a la privacidad. Debe lograrse un equilibrio adecuado para que la autoridad de competencia pueda ejercer plenamente sus facultades sin necesidad de entrometerse en el funcionamiento de la empresa ni en la vida personal de los empleados.

79. Por otra parte, la adopción de herramientas digitales podría requerir cierta adaptación y cierta coordinación interna de los recursos presupuestarios y humanos y una colaboración externa con organismos gubernamentales u otras autoridades para garantizar su máximo aprovechamiento. Esto podría requerir una cantidad considerable de recursos, para lo cual se necesita una planificación y un diseño adecuados de las estrategias más rentables que sean apropiadas para una autoridad de competencia concreta en función del entorno en que lleve a cabo sus actividades.

80. Los diversos desafíos existentes y la necesidad de aprovechar al máximo las oportunidades que ofrece la digitalización también ponen de manifiesto la importancia de la cooperación internacional entre autoridades de competencia para intercambiar experiencias y mejores prácticas sobre la adopción y el empleo de herramientas digitales de un modo que minimice el riesgo de desafíos y que sea el más adecuado y eficaz.

Notas finales

[1] OCDE (2020), *Panorama de las Administraciones Públicas: América Latina y el Caribe 2020*, OECD Publishing, París, https://www.oecd-ilibrary.org/governance/panorama-de-las-administraciones-publicas-america-latina-y-el-caribe-2020_1256b68d-es, p. 12.

[2] *The Economist*, «Rigging the Bids», 19 de noviembre de 2016, https://www.economist.com/europe/2016/11/19/rigging-the-bids.

[3] OCDE (2013), «Ex-officio Cartel Investigation and the Use of Screens to Detect Cartels», https://www.oecd.org/daf/competition/exofficio-cartel-investigation-2013.pdf.

[4] OCDE (2016), «Promoviendo la competencia efectiva en los procesos de compras públicas», http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/LACF(2016)31&docLanguage=Es.

[5] OCDE (2018), «Workshop on cartel screening in the digital era», https://www.oecd.org/competition/workshop-on-cartel-screening-in-the-digital-era.htm.

[6] OCDE, «Summary of the workshop on cartel screening in the digital era», 30 de enero de 2018, https://one.oecd.org/document/DAF/COMP/M(2018)3/en/pdf.

[7] OECD (2013), «Visitas de inspecciones sin previo aviso en investigaciones de conductas anticompetitivas», http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/LACF(2013)6&docLanguage=Es.

[8] OCDE (2018), «Investigative Powers in Practice: Unannounced Inspections in the Digital Age», https://one.oecd.org/document/DAF/COMP/GF(2018)7/en/pdf.

[9] OCDE (2019), Council Recommendation concerning Effective Action against Hard Core Cartels, https://www.oecd.org/daf/competition/recommendationconcerningeffectiveactionagainsthardcorecartels.htm.

[10] La realización de imágenes forenses es un proceso a través del cual se copian todos los datos contenidos en un suporte de almacenamiento, incluido el espacio no asignado. También se denomina «replicación», puesto que se crea una réplica del contenido del soporte.

[11] En la práctica existen varios programas de *software* que se utilizan para las técnicas forenses digitales, entre los que destacan *EnCase* y *Nuix* como los más populares, utilizados por diversas autoridades de competencia. Sin embargo, no todas las autoridades utilizan herramientas forenses, y en esos casos se copian las fuentes digitales de pruebas a través de herramientas de búsqueda integradas y se recuperan y copian los datos eliminados desde la «papelera» o desde servidores de copias de seguridad.

[12] Las técnicas forenses en tiempo real consisten en incautar o analizar información de sistema, contenidos de la memoria o contenidos de soportes de datos a partir de sistemas en tiempo real (es decir, sistemas que están en funcionamiento). De ese modo se extrae información de la memoria en uso (es decir, información que se pierde cuando los dispositivos o sistemas informáticos no están en funcionamiento o están apagados) (RIC, 2014, p. 6).

[13] La cadena de pruebas es un registro de las actividades de incautación, análisis o tratamiento de las pruebas digitales que demuestra claramente que las pruebas se han extraído de la información digital incautada. En la mayoría de las jurisdicciones, para que las pruebas digitales sean jurídicamente admisibles se debe disponer de un documento válido que justifique su autenticidad, o bien de pruebas de que son idénticas a la información digital incautada. La cadena de custodia es el registro del historial de custodia de las pruebas. En la mayoría de las jurisdicciones, para que las pruebas sean jurídicamente admisibles ante un tribunal es necesario que exista un registro válido de la cadena de custodia o una descripción de quiénes han estado en posesión física de ellas, por qué y dónde (RIC, 2014, p. 5).

[14] Un valor de *hash* es un valor numérico único que sirve para identificar los datos, como si de una huella digital se tratase. Se genera mediante algoritmos matemáticos. Los datos no pueden modificarse sin cambiar el valor de *hash* correspondiente. Si alguien modifica posteriormente un solo punto del contenedor de los datos, este cambio alterará

el valor de *hash*. Por lo tanto, está garantizado que, mientras el valor de *hash* siga siendo el mismo, el contenedor contiene los mismos datos.

[15] La REC (2013, p. 4) recomienda el procedimiento de inspección continuada como una manera eficaz de obtener pruebas digitales. Este procedimiento ofrece más tiempo para seguir analizando los datos y entender mejor el caso, de modo que aumenta las posibilidades de detectar pruebas pertinentes en el a menudo voluminoso expediente digital. Además, este procedimiento reduce al mínimo la perturbación de las operaciones de la empresa. Sin embargo, también se ha señalado que copiar y llevarse una gran cantidad de datos para su examen o cribado podría suponer una violación de derechos básicos como la privacidad o del privilegio jurídico de la empresa investigada (OCDE, 2018a, p. 6).

[16] Véase https://www.globallegalinsights.com/practice-areas/cartels-laws-and-regulations/chile.

[17] A modo de ejemplo, lo normal es que en Alemania, Australia, Austria, Chile, Francia y Rumanía se requiera una orden judicial para las investigaciones sorpresivas.

[18] Tribunal de Justicia de la Unión Europea, C-37/13 P, Nexans SA y Nexans France Sas contra Comisión Europea, 25 de junio de 2014, ECLI:EU:C:2014:2030, párr. 33.

[19] Parr, «GC Nexans: EC seizure of electronic data in raids under scrutiny», 21 de marzo de 2017, https://app.parr-global.com/intelligence/view/prime-2403799.

[20] Conclusiones de la Abogada General Sra. J. Kokott en C-606/18 P, Nexans France y Nexans contra Comisión Europea, 12 de marzo de 2020, ECLI:EU:C:2020:207, párr. 77.

[21] Directiva (UE) 2019/1 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, encaminada a dotar a las autoridades de competencia de los Estados miembros de medios para aplicar más eficazmente las normas sobre competencia y garantizar el correcto funcionamiento del mercado interior, DO L 11 de 14 de enero de 2019, pp. 3 a 33.

[22] Conclusiones de la Abogada General Sra. J. Kokott en C-606/18 P, Nexans France y Nexans contra Comisión Europea, 12 de marzo de 2020, ECLI:EU:C:2020:207, párr. 59.

[23] Comisión Europea, Nota explicativa sobre inspecciones de la Comisión de conformidad con el artículo 20, apartado 4, del Reglamento n.º 1/2003, 11 de septiembre de 2015, apartado 16.

[24] El actual proyecto de Recomendación del Consejo de Transparencia y Equidad Procesal en la Aplicación de las Leyes de Competencia de la OCDE, de 28 de mayo de 2020 (DAF/COMP/WP3/WD(2020)23), recomienda que la autoridad de competencia establezca unos sistemas de control de los distintos pasos del proceso internos adecuados con el fin de garantizar la legalidad, la proporcionalidad y la coherencia.

[25] Véanse, sobre este punto, Tribunal de Justicia de la Unión Europea, C-46/87 y 227/88, Hoechst AG contra Comisión, 21 de septiembre de 1989, ECLI:EU:C:1989:337, párr. 15; Tribunal de Justicia de la Unión Europea, C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P y C-219/00 P, Aalborg Portland y otros contra Comisión, 7 de enero de 2004, ECLI:EU:C:2004:6, párr. 63; y Tribunal General, T-135/09, Nexans France y Nexans contra Comisión, 14 de noviembre de 2012, ECLI:EU:T:2012:596, párr. 41.

[26] Conclusiones de la Abogada General Sra. J. Kokott en C-606/18 P, Nexans SA y Nexans contra Comisión Europea, 12 de marzo de 2020, ECLI:EU:C:2020:207, párr. 62.

[27] Conclusiones de la Abogada General Sra. J. Kokott en C-606/18 P, Nexans SA y Nexans contra Comisión Europea, 12 de marzo de 2020, ECLI:EU:C:2020:207, párrs. 82 y 83.

[28] Comisión Europea, Nota explicativa sobre inspecciones de la Comisión de conformidad con el artículo 20, apartado 4, del Reglamento n.º 1/2003, apartado 10.

[29] Indecopi, «Proyecto de Lineamientos de Visitas de Inspección», octubre de 2019, https://www.indecopi.gob.pe/documents/51771/2962929/Lineamientos+de+Visitas+de+Inspecci%C3%B3n/, pp. 34 y 35.

[30] CNMC, Decisión R/0148/13, Renault, 23 de septiembre de 2013, https://www.cnmc.es/sites/default/files/364802_17.pdf, p. 8.

[31] Juan David Gutiérrez, «Proposal for the Publication of a Guide to Regulate "Dawn Raids" by the Colombian Competition Authority», *Competition Policy International*, junio de 2020,

https://www.competitionpolicyinternational.com/proposal-for-the-publication-of-a-guide-to-regulate-dawn-raids-by-the-colombian-competition-authority/.

[32] Parr, «Croatian authority fines fourteen driving schools for cartel», 23 de marzo de 2020, https://app.parr-global.com/intelligence/view/prime-3006225 y https://www.aztn.hr/en/driving-schools-price-fixing-cartel/. Véase también Merve Bakırcı, «Turkey: Obtaining And Examining WhatsApp Correspondences As Evidence Within The Scope Of Competition Law», *Mondaq*, 19 de noviembre de 2019, https://www.mondaq.com/turkey/antitrust-eu-competition-/865588/obtaining-and-examining-whatsapp-correspondences-as-evidence-within-the-scope-of-competition-law.

[33] OCDE (2019), Council Recommendation concerning Effective Action against Hard Core Cartels, https://www.oecd.org/daf/competition/recommendationconcerningeffectiveactionagainsthardcorecartels.htm.

[34] Véase, por ejemplo, el caso de Canadá, donde los investigadores de la autoridad de competencia han descargado datos ubicados fuera del país en el marco de registros de sistemas informáticos situados en Canadá, si bien sigue habiendo cierta controversia en cuanto a los límites concretos de la autoridad concedida mediante una orden que autoriza el registro de sistemas informáticos en un contexto transfronterizo (https://www.lexology.com/gtdt/tool/workareas/report/617528c4-0e23-4678-a460-9333ed458dc0).

[35] Para obtener más información, véanse http://www.oas.org/juridico/english/cyb20_network_en.pdf y http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf.

[36] Por ejemplo, en algunos casos, el equipo informático forense permitió que los investigadores recuperaran correos electrónicos que los empleados de la empresa investigada habían eliminado de manera deliberada (OCDE, 2018d, p. 4 (UE) y OCDE, 2018f, p. 5 (Corea)).

[37] Para obtener más información, véase la mesa redonda de la OCDE sobre «Improving International Co-operation in Cartel Investigations», http://www.oecd.org/daf/competition/ImprovingInternationalCooperationInCartelInvestigations2012.pdf.

[38] Véase https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2012_ISEC_FP_C2_4000003977_en.

[39] Véase https://www.kkv.fi/ajankohtaista/ura-kkvssa/mita-kkv-tekee/tietotekninen-tutkinta/.

Referencias

Ardiyok, S. and B. Yüksel (2016), "The Use of Digital Evidence and Technological Tools in Competition Enforcement Actions and their Interference with Private and Privileged Information and Data Protection Rules", https://www.mondaq.com/turkey/trade-regulation-practices/479716/the-use-of-digital-evidence-and-technological-tools-in-competition-enforcement-actions-and-their-interference-with-private-and-privileged-information-and-data-protection-rules.

Connor, M. (2014), "Price-Fixing Overcharges: Revised 3rd Edition", https://ssrn.com/abstract=2400780.

Connor, J. (2016), "The Private International Cartels (PIC) Data Set: Guide and Summary Statistics, 1990- July 2016", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2821254.

ECN (2013), "ECN Recommendation on the Power to Collect Digital Evidence, including by Forensic Means", https://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf.

European Commission (2015), "Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003", https://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf.

European Commission (2016), "Public consultations on Empowering the national competition authorities to be more effective enforcers – Note of the French Competition Authority", https://ec.europa.eu/competition/consultations/2015_effective_enforcers/french_authorities_fr.pdf.

Harrington, J. E. (2007), "Behavioral Screening and the Detection of Cartels", In: *Enforcement of the Prohibition of Cartels (Ehlermann C.-D. and I. Atanasiu eds.)*, European Competition Law Annual 2006, Oxford, https://unctadcompal.org/wp-content/uploads/2017/11/Lectura-8-Handbook-Bucirossi-Cap-6.pdf.

ICN (2014), "Anti-Cartel Enforcement Manual Chapter 3: Digital Evidence Gathering", https://www.internationalcompetitionnetwork.org/portfolio/digital-evidence-gathering.

Imhof, D., Y. Karagök and S. Rutz (2018), "Screening for Bid Rigging – Does It Work?", *Journal of Competition Law & Economics*, Volume 14, Issue 2, pp. 235–261, https://doi.org/10.1093/joclec/nhy006.

Ivaldi M., F. Jenny, and A. Khimich (2016), "Cartel Damages to the Economy: An Assessment for Developing Countries", in Jenny F. and Y. Katsoulacos (eds.), *Competition Law Enforcement in the BRICS and in Developing Countries*, Springer, pp. 103–133.

Michalek, M. (2015), *Right to Defence in EU Competition Law: The case of Inspections*, University of Warsaw Faculty of Management Press, https://www.cars.wz.uw.edu.pl/tresc/ksiazki/31/CARS18_Michalek.pdf.

OECD (2020), *OECD Peer Reviews of Competition Law and Policy: Mexico,* http://www.oecd.org/daf/competition/Mexico-Peer-Reviews-of-Competition-Law-and-Policy-en.pdf.

OECD (2020a), Criminalisation of cartels and bid rigging conspiracies: a focus on custodial sentences, https://one.oecd.org/document/DAF/COMP/WP3(2020)1/en/pdf.

OECD (2020b), Competition Trends 2020, https://www.oecd.org/daf/competition/OECD-Competition-Trends-2020.pdf.

OECD (2019), *OECD Peer Reviews of Competition Law and Policy: Brazil*, http://www.oecd.org/daf/competition/oecd-peer-reviews-of-competition-law-and-policy-brazil-ENG-web.pdf.

OECD (2018a), "Investigative Powers in Practice: Unannounced Inspections in the Digital Age", https://one.oecd.org/document/DAF/COMP/GF(2018)7/en/pdf.

OECD (2018b), "Summary of the workshop on cartel screening in the digital era", https://one.oecd.org/document/DAF/COMP/M(2018)3/en/pdf.

OECD (2018c), "Investigative Power in Practice – Contribution from Mexico (COFECE)", https://one.oecd.org/document/DAF/COMP/GF/WD(2018)28/en/pdf.

OECD (2018d), "Investigative Power in Practice – Contribution from the European Commission", https://one.oecd.org/document/DAF/COMP/GF/WD(2018)25/en/pdf.

OECD (2018e), Annual Report on Competition Policy - Developments in Portugal, https://one.oecd.org/document/DAF/COMP/AR(2018)13/en/pdf.

OECD (2018f), "Investigative Power in Practice – Contribution from Korea", https://one.oecd.org/document/DAF/COMP/GF/WD(2018)63/en/pdf.

OECD (2018g), "Investigative Power in Practice – Contribution from South Africa",

https://one.oecd.org/document/DAF/COMP/GF/WD(2018)37/en/pdf.

OECD (2018h), "Investigative Power in Practice – Contribution from Australia", https://one.oecd.org/document/DAF/COMP/GF/WD(2018)18/en/pdf.

OECD(2018i), "Investigative Power in Practice - Contribution from Peru, https://one.oecd.org/document/DAF/COMP/GF/WD(2018)66/en/pdf.

OECD (2017), "Algorithms and Collusion - Note from the United Kingdom", https://one.oecd.org/document/DAF/COMP/WD(2017)19/en/pdf.

OECD (2016), "Fighting bid rigging in public procurement: Report on implementing the OECD Recommendation", https://www.oecd.org/daf/competition/Fighting-bid-rigging-in-public-procurement-2016-implementation-report.pdf.

OECD (2013), "Ex Officio Cartel Investigations and the Use of Screens to Detect Cartels", http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP(2013)14&docLanguage=En.

OECD (2013a), Unannounced Inspections in Antitrust Investigations, DAF/COMP/LACF(2013)6, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/LACF(2013)6&docLanguage=En.

Scordamaglia-Tousis, A. (2013), EU Cartel Enforcement: Reconciling Effective Public Enforcement with Fundamental Rights, Kluwer Law.

Smuda, F. (2015), "Cartel Overcharges and the Deterrent Effect of EU Competition Law", *Centre for European Economic Research Discussion Paper*, http://ftp.zew.de/pub/zew-docs/dp/dp12050.pdf.

Van Erps, D. (2013), "Digital evidence gathering: An update – The EC Practice", *Concurrences N° 2-2013, Art. N° 52014, pp. 213-219,* https://www.concurrences.com/en/review/issues/no-2-2013/legal-practice/digital-evidence-gathering-an-update.