Organisation for Economic Co-operation and Development

DAF/COMP/LACF(2020)2

Unclassified

English - Or. English

5 August 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

LATIN AMERICAN AND CARIBBEAN COMPETITION FORUM - Session I: Digital Evidence Gathering in Cartel Investigations

- Issues Note -

28-29 September 2020

This document was prepared by the OECD Secretariat to serve as an Issues note for the discussion on *Digital Evidence Gathering in Cartel Investigations* that will take place at the Latin American and Caribbean Competition Forum on 28-29 September 2020 via virtual zoom meeting.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

More documentation related to this discussion can be found at oe.cd/laccf.

Please contact Ms. Cristina Volpin [E-mail: Cristina.Volpin@oecd.org] or Lynn Robertson if you have any questions about this document [E-mail: Lynn.Robertson@oecd.org].

JT03464446

LATIN AMERICAN AND CARIBBEAN COMPETITION FORUM - Session I: Digital Evidence Gathering in Cartel Investigations

– Issues Note by the Secretariat[*] –

ABSTRACT

Companies increasingly recur to digital communications and storage of documents. The change brought by digitalisation to the way in which companies operate creates opportunities but also a number of challenges for competition enforcement.

Competition authorities may adopt a number of digital tools and resources to strengthen their fight against cartels, which may allow them to search through high volumes of data in a swift manner and with a high degree of accuracy. However, the implementation of these tools may not always be straightforward. A few legal and practical challenges may arise in relation to the protection of the authenticity of the seized evidence and of the rights of defence of the company and its employees. In addition, internal coordination of resources and external co-operation may need to be implemented to ensure the full exploitation of the opportunities offered by these tools.

This Issues Note will discuss some advantages and disadvantages of the most common digital tools for evidence gathering, and it will explore some of the legal and practical issues arising from their use, drawing from cases where competition authorities across the world dealt with the delicate phase of evidence gathering in cartel enforcement.

[*] This Issues Note was prepared by Harry Hong, Takuya Ohno and Cristina Volpin of the OECD Competition Division and it benefitted from comments by Antonio Capobianco, Lynn Robertson and Sabine Zigelski.

Table of contents

Boxes

1. Introduction

1. Cartels are considered the most serious infringement of competition law and the harm caused by cartels is very significant. The median cartel price overcharge in the EU and in some developing countries is estimated at 20% and only slightly lower (between 16.7% and 19%) in the US and Canada (Ivaldi et al., 2016, p. 8; Smuda, 2015; Connor, 2014). Between 1990 and 2016, over 100.000 companies were involved in cross-border price-fixing. The gross cartel overcharges during that period have been calculated to exceed USD 1.5 trillion and the amount of sales affected by international cartels exceeded in nominal terms USD 50 trillion (Connor, 2016).

2. Public procurement may also be particularly prone to cartel behaviour in the form of bid rigging. The negative impact on the public is particularly important given the size of public procurement spending. In 2017, public procurement represented 6% of GDP on average in Latin America and the Caribbean region. However, one third of the countries in this region have not yet adopted electronic government procurement systems, which may allow more transparency and efficiency.[1] While estimations are difficult, collusive tendering has been considered to increase costs by 2% to 15% depending on the industry affected.[2]

3. Given its consequences, the discovery, investigation and prosecution of cartel conduct is an enforcement priority of many competition authorities, in OECD countries and across the world (OECD, 2020a, p. 5). In 2018, authorities in 49 countries took an average of around 10 cartel decisions and an average of 6 in the Americas (OECD, 2020b, p. 28).

4. The changes brought about by digitalisation have transformed law enforcement in many sectors, including competition law. Companies communicate internally and externally via digital means and increasingly create, store and process information in digital format. Accordingly, competition authorities are required to adjust their investigative tools to these changes and increasingly utilise digital tools in the detection and gathering of evidence of cartel conduct.

5. For instance, an important role in the detection of cartel is played by data screening tools. The use of cartel screens has been discussed in a roundtable on Ex-officio Cartel Investigation and the Use of Screens to Detect Cartels in 2013,[3] in a LACF session on Promoting effective competition in public procurement in 2016[4] and, more recently, in an OECD Workshop on Cartel Screening in the Digital Era in 2018.[5]

6. Often, a combination of sophisticated software and simpler statistical methods and the use of structural and behavioural approaches will be adopted by competition authorities in cartel screening. Given that screens are mainly applied to collusive tendering, digitalisation of private businesses and public administrations and the increased availability of data in digital form contributes to facilitating the detection of anticompetitive bids.[6]

7. Other digital tools support the gathering of digital evidence in cartel enforcement. Digital forensics, in particular, is increasingly used by competition authorities for the copying and analysis of evidence found during inspections and to deal with very large amount of data in an efficient manner. The importance of these tools has also been increased by the Covid-19 pandemic, which, due to social distancing limitations and teleworking measures, limited the ability of competition authorities of conducting unannounced inspections and on-site interviews, and has further increased the importance of tools that allow the analysis of evidence at a location that is different from the companies' premises.

8. Whilst they provide great opportunities for evidence gathering and investigation, however, the use of digital tools in cartel enforcement may raise a few legal and practical challenges.

9. Legal challenges may vary significantly depending on the legal regime in each jurisdiction. Three main legal challenges are, however, commonly identified across jurisdictions with respect to the collection of evidence via digital tools. The first one is the limitation of the scope of the investigation to what is considered proportional, given that digital tools allow the copying of large volumes of data at high speed. A second, related issue arises in relation to the interplay between access to personal electronic devices and data storage systems that may be kept at work or contain work-related information and the right to privacy. A third issue arises in connection to the location of digital information and whether, if they are not located at the business premises, searching them may go beyond the scope of the judicial warrant or competition authority's order. Depending on the legal framework, some or all of these legal issues, if not dealt with correctly by competition officials, may result in procedural irregularities that may be raised in court.

10. Practical challenges in relation to the adoption and use of digital tools for evidence gathering in cartel proceedings may also arise in relation to the administration of resources, capacity-building, and internal and external co-operation.

11. First, the above-mentioned digital tools are quite resource intensive, in terms of specific expertise, equipment and infrastructure. This may be costly for competition authorities, which may need to choose the most appropriate ways of adopting these tools depending on their budget constraints or other limitations (e.g. availability of IT support or physical space), but also human resource-intensive, because it may require hiring specialists, creating a dedicated internal unit, or setting up of collaboration with external experts (e.g. computer and data scientists).

12. Second, co-operation with other national bodies or with other competition authorities may be necessary or useful (for instance, in bid rigging cases or in cross-border cartels) for digital evidence gathering. Establishing these kinds of co-operations may be complex but competition authorities may considerably benefit from exploiting the opportunities they offer.

13. Some of these issues have been touched upon, but have not been explored in details in the 2013 LACF session on Unannounced Inspections in Antitrust Investigations[7] and in the 2018 Global Forum on Competition session on Investigative Powers in Practice: Unannounced Inspections in the Digital Age.[8] In addition, the 2019 Council Recommendation concerning Effective Action against Hard Core Cartels explicitly refers to the importance for competition authorities of having effective powers to investigate hard core cartels and, among others, the power to:

> *Access electronic information that could help establish a cartel violation including electronic material that is stored remotely (e.g. on 'the cloud') and have access to appropriate investigative techniques, such as communications interception and surveillance authorisations. For this purpose, competition authorities should have trained specialised staff and adequate hardware and software equipment.*[9]

14. The present Issues Note aims at analysing the benefits and the challenges faced by competition authorities when adopting specific tools for digital evidence gathering in cartel enforcement. Section 2 will describe the collection, preservation and analysis of digital evidence by means of forensic IT tools and their functioning. Section 3 will deal with the main legal challenges associated with the digital evidence gathering in cartel investigations. Section 4 will describe the reorganisation of budgetary or human resources, including the delivery of dedicated digital staff training for the adoption of digital evidence gathering

tool. It will also explore the importance of setting up national or international collaboration aimed at collecting evidence in this area and the challenges arising from it.

2. Digital Evidence Gathering Methods in Cartel Investigation

15. An increasing number of competition authorities include digital data in their inspections to find relevant evidence. Due to the increasing volume of digital data and the complexity of fast changing IT environments, finding evidence during an on-site inspection has become an arduous task. Modern IT systems, such as cloud computing, may be cost-efficient and make it easy to store and retrieve data for firms but they may also create more technical and legal difficulties for the investigators and prosecutors to access the firm's electronic data and gather meaningful evidence.

16. Accordingly, several competition authorities use advanced digital tools and techniques during their investigation and evidence gathering procedures. The methods and procedures adopted by the competition authorities differ depending on their resources (e.g. equipment, software, trained staff) and the relevant legal framework.

2.1. Collection of digital evidence

17. In unannounced inspections, digital data is collected mainly in two ways. The first is the physical seizure of the data carriers such as hard drives, CDs and USB sticks to be later searched for relevant evidence at the premises of the competition authority.

18. The second way is searching the data carriers at the premises of the inspected undertaking and copying or making forensic images[10] of the digital data. Forensic IT tools are used to collect digital evidence.[11] Some authorities also engage in live forensics[12] to capture volatile data which cannot be accessed once the device is turned off. (OECD, 2018a, p. 5)

19. Some measures should be taken by the inspection teams to ensure the integrity of the data and to enable authentication. In order to establish authenticity of digital evidence, it is crucial to maintain a chain of evidence and chain of custody.[13] Activities relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review. This record of all processes applied to digital evidence should be available to an independent third party to examine the original data following the same steps and to reach the same results. In practice, for instance, when imaging data carriers, write blockers are used to secure the integrity of the source media. Also, hash values[14] of every copied/imaged data should be generated and saved to enable verification that the copy is identical to the original digital information. It is also important to document every action during this process.

20. At the end of the inspection, non-relevant digital information is either returned to the company or deleted permanently. For the latter, the inspectors should completely wipe all forensic IT tools on which company data have been stored (the so-called "sanitization" process). The goal of sanitising is to completely remove the data from a storage device in a way that the data cannot be reconstructed. Typically, the equipment is wiped with traditional wiping tools in a single wipe implying that the complete surface of mechanical hard drives will be overwritten with a certain pattern. (European Commission, 2015, p. 3; ICN, 2014, p. 21; Van Erps, 2013, p. 214)

21. Once digital data gathered at the premises have been preliminarily inspected, some authorities have the power to transport the data to their premises (or to premises of the police or of an equivalent enforcement authority) to continue searching of evidence. It typically happens when inspectors cannot finish the searching and collecting on the spot because the device was identified relatively late in the course of the inspection, technical problems arose or when the operations would last too long putting a disproportionate burden on inspected firms' daily business. This procedure is called "continued inspection" procedure.[15] In some jurisdictions, the selection of the digital evidence may be conducted on a *prima facie* basis at the premises of the inspected company (for example, by performing searches using keywords) with further review and selection will later take place at the premises of the authority. Some authorities routinely take a forensic image of the storage media at the inspection and carry out the review of the data later at their premises, whereas others do so on a case-by-case basis. (ECN, 2013, p. 3; OECD, 2018a, p. 6; Van Erps, 2013, p. 214) The potential legal challenges arising in connection with this procedure are discussed in Section 3.

2.2. Preservation of digital evidence

22. Some measures should be taken for the preservation of the digital evidence seized during the inspection. Preservation means the prevention of deletion or destruction of the digital evidence during the inspection, transportation and analysis (see also Box 1).

Box 1. Alteration or destruction of digital evidence

Although the issue of the alteration or destruction of digital evidence by the parties during surprise inspection is not specific to digital evidence, digital evidence may be moved, altered or destroyed in an easy and faster way than physical evidence. As noted by a former Vice President of the European Commission, Joaquín Almunia:

> *"Company information is nowadays essentially stored in IT environments like email systems and can be quickly modified or deleted. This decision sends a clear message to all companies that the Commission will not tolerate actions which could undermine the integrity and effectiveness of our investigations by tampering with such information during an inspection."*

Whilst attempts to hide, alter or destroy digital evidence may be counteracted by specific tools that allow to retrieve and restore it, they may significantly disrupt the efforts of the competition authority and hinder its search. To discourage these attempts, it is important that competition authorities enjoy power to impose significant and adequately deterrent fines.

In December 2019, for instance, the Netherlands Authority for Consumers and Markets (ACM) imposed a fine of 1.84 million Euros on a company whose employees deleted WhatsApp conversations and left some WhatsApp groups during on-the-spot inspection. It also restated the duty to co-operate on the investigated companies by giving accurate information and granting access to the relevant documents and the obligation not to destroy, withhold or dispose of evidence before and during an unannounced inspection.

In an earlier case in 2012, the European Commission had fined two Czech energy companies, Energetický a průmyslový holding a.s. and EP Investment Advisors s.r.o., for not having blocked an email account as requested and having diverted incoming emails. This action was considered a procedural infringement by the General Court, which also clarified that "*the Commission has the burden of proving that access was granted to the data in Mr M.'s blocked e-mail account, but is not required to prove that those data were manipulated or deleted*."

Source: European Commission, Press Release of 28 March 2012, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_319.
ACM, Press Release of 11 December 2019, https://www.acm.nl/en/publications/acm-has-imposed-fine-184-million-euros-deleting-whatsapp-chat-conversations-during-dawn-raid.
General Court of the European Union, Case T-272/12, Energetický a průmyslový holding a.s. and EP Investment Advisors s.r.o. v European Commission, 26 November 2014, EU:T:2014:995, para. 39.

23. Preservation measures include leaving devices running for live forensics, requesting blocking access to mailboxes at the server level, unplugging network cables from the computers to avoid unauthorized access, recording user attribution evidence (to identify whom the user is, if later contested, and whether others may be logged onto the computer), protecting data carriers from static electricity, magnetic fields and concussions. Furthermore, processing working copies of the digital data is a widely accepted measure to avoid accidental harm to the original digital data. As mentioned before, maintaining a sound chain of custody until the closure of the case is also crucial. (ICN, 2014, p. 22; OECD, 2018a, p. 6)

2.3. Analysis of digital evidence

24. After the data collection phase, the case team or/and forensics experts analyse the data to find pieces of evidence. Since digital searches can yield huge amounts of data, some kind of search strategy needs to be developed.

25. Keyword searching is the most used method. Keywords are derived from desk research, informants, leniency applicants or explanations sought during the on-the-spot inspection. As analysis progresses, new keywords can be added to the list. Specially developed forensic search software such as *EnCase* and *Nuix* can identify misspelled versions of the keywords and yield more comprehensive results, as well as produce results on the basis of self-learning algorithms.

26. Moreover, these types of forensic software allow "concept" searching, which is much more developed when compared to basic keyword searches. Concept searching detects synonyms and misspellings, identifies variations of certain keywords, identifies groups which consists of people that regularly communicate with each other and track communications on different applications (e.g. instant messaging applications) and automatically crosschecks the content of communications within the groups with keywords and the variations of these keywords. These tools make it much easier for the authorities to find relevant evidence (Ardiyok and Yüksel, 2016; Van Erps, 2013, p. 214).

27. Other analytical methods are confirming user attribution, viewing the print spooler, testing file signatures to find bad file signatures, searching for encrypted information, investigating traces of web chats, webmail and so on. Applying more than one method to the data can minimise the risk of false negatives (ICN, 2014, p. 24; OECD, 2018a, p. 7).

28. It is again important to document all the action taken to extract the evidence to maintain chain of evidence, to enable third parties to reproduce the same results (OECD, 2018a, p. 7).

Box 2. Digital Evidence Gathering Procedure in the European Union

1. On-the-spot selection procedure

Making a forensic copy: inspectors extract possible relevant files (information in certain folders or certain document types) from the target device by making a forensic copy of the content. Once a forensic copy is made, inspectors may return the target device to the inspected company.

Uploading/Indexing/Reviewing the forensic copy: the copy of all the potentially relevant information will be uploaded on the European Commission's server. All the uploaded data will then be indexed, which means that all the information is catalogued. Once it is indexed, the data will be reviewed by officials on review stations.

Tagging and copying: when officials identify relevant data, these will be "tagged". The collection of relevant data will then be copied on an encrypted data carrier (DVD, USB stick or hard disk) together with a list that contains the name, the path and a hyperlink to the document. A separate file on the data carrier mentions the "hash value" of the container that contains all the data. The document list is signed by a representative of the undertaking and an official. The undertaking receives a copy of the data carrier with the data and the list.

2. Sanitising equipment procedure

At the end of the inspection, the officials sanitise all the European Commission equipment that has been used to store digital information of the company before leaving the undertaking.

3. Continued inspection procedure

The information that is considered potentially relevant on the basis of a preview or in view of search results relating to other data from the same custodian will be put on a storage medium and encrypted. The officials put the storage medium in a sealed envelope and make a copy for the undertaking.

Then the sealed envelope is taken back to the European Commission which commits to return the sealed envelope to the undertaking or to invite the undertaking to attend the opening of the sealed envelope at the European Commission premises and assist in the continued selection process. The relevant documents will be identified, as described above ("tagged", copy on data carrier together with list), the undertaking receives a copy and the storage medium will be sanitised.

Source: Van Erps (2013)

Box 3. Open Issues

1. What are the most effective digital tools for evidence gathering in cartel investigation?
2. What are the most significant benefits of using digital tools in evidence gathering?
3. What difficulties did you encounter in applying them?
4. In which cartel cases were digital tools most useful for gathering evidence?

3. Legal challenges of digital evidence gathering in cartel investigations

29. The use of digital tools increases the chances that competition authorities detect cartels and gather relevant information in their investigations, since digital tools allow competition authorities to access a wider variety of evidence and to seize larger amount of documents.

30. However, precisely due to these broadened possibilities, some legal challenges may arise in relation to the adoption of these tools due to tensions between the need of the competition authority to conduct a thorough investigation and due process safeguards. As mentioned above, legal challenges may vary based on the relevant legal regime. Competition authorities across the world, however, are confronted with some common challenges in relation to the gathering of digital evidence in cartel cases and the exercise of their powers of investigations. Some of the main ones are addressed below.

3.1. Proportionality of the investigation

31. Typically, unannounced inspections need to be targeted, meaning that at the time of the inspection order, the competition authority has to have reasonable grounds justifying the inspection. The inspection should have the purpose of verifying whether a particular suspicion is founded or whether *prima facie* evidence of an infringement may find corroboration. Unannounced inspection should not be 'fishing expeditions', whereby the competition authorities looks for reasons to investigate an infringement. These reasons must pre-exist.

32. In many countries, a decision of the competition authorities is sufficient to conduct an inspection of business premises, but a judicial order may be required if the parties deny access to the premises (for instance, Peru) (OECD, 2018i, p. 4) or for the inspection of private domicile. In other countries (like Chile),[16] a court warrant is required for the inspection of business premises.[17] A judicial warrant or an inspection order must usually provide details of the alleged facts that require verification, including the subject matter of the investigation, its purpose and any potential penalties that may derive from the lack of co-operation by the company throughout the investigation.

33. One important advantage of digitalisation is the fact that high volumes of data and information can be analysed and copied swiftly. Whilst the power of the competition authorities to make digital copies and collect electronic evidence is fundamental for the conduct of investigation in a digitalised work, the modalities of its exercise may differ. As mentioned in Section 2, some authorities can make digital copies of evidence for *in situ* inspection, whilst other can seize devices or take copies to examine at their offices.

34. The question arises therefore whether competition authorities have the discretion to seize a larger amount of document and data that may strictly be relevant to the investigation, in order to analyse them at the competition authority's premises in a second moment and make copies only of those that are found relevant for them to be added to the file.

35. Even if, with the aid of the above-described forensic tools, competition authorities are likely to conduct extremely thorough searches, determining on the spot what documents and files should be copied may still be lengthy and may heighten the risk that something may be missed. The competition authority should be endowed with the inspection powers that allow it to "*perform its task of protecting the […] market from distortions of competition and to penalise any infringements of the competition rules on that market*".[18] In addition, the ability to copy data for later examination is also a way to minimise the intrusion for the company and to protect the integrity of the data copied.[19]

36. As noted by the Mexican authority COFECE (OECD, 2018c), which has the power to copy entire hard drives and other digital evidence, but cannot examine evidence at its premises:

> *The main challenge the Commission faces when conducting dawn raids is that […] [f]or example, it cannot seize computers, documents or information (it can only copy them). This implies that the Investigative Authority's dawn raids absorb plenty of the Commission resources since it cannot simply take relevant physical documents and electronic devices for further analysis at the Commission headquarters. The team must copy these documents and devices which takes significantly more time and resources*. (OECD, 2018c, p. 7)

37. Advocate-General Kokott in the *Nexans* case pending before the Court of Justice of the European Union also stated:

> *Particularly in the light of the volume of electronic data produced and stored by undertakings […], it […] appears perfectly justified to permit the Commission to carry out the time-consuming examination of such data at its own premises so as not to tie Commission staff unduly to the premises of the undertakings being inspected, which may also give rise to high costs.*[20]

38. In the EU, the power "*to take or obtain, in any form, copies of or extracts from such books or records and, where they consider it appropriate, to continue making such searches for information and the selection of copies or extracts at the premises of the national competition authorities or at any other designated premises*" has now been expressly recognised by Article 6(1)(c) of the ECN+ Directive, which will have to be transposed by the EU Member States by 4 February 2021.[21]

39. In other jurisdictions, it may be a question of judicial interpretation whether the powers bestowed upon the authority by the law will include the gathering of digital evidence, which is typically not expressly referred to by older legislation, and what the boundaries of this power are. However, this power may be extremely important for the conduct of investigations by competition authorities, and, when adequate guarantees are undertaken, the fact that the data have been examined after having been copied should not raise legitimacy issues. To this purpose, it is particularly important that the inspection order contains a clear and thorough indication of the reasons for the inspection, the matter to which the investigation pertains, and the evidence sought, and that the documents and files seized and placed in the case file are considered, based on these parameters, relevant to the investigation.[22]

40. An examination of data at the premises of the competition authority, may, therefore, be justified, due to, for instance, i) the large volume of data to be analysed; ii) the fact that the on-the-spot examination would otherwise be prolonged over multiple days, or iii) the fact that the examination of specific devices had to be postponed (for instance, due to absence of the computer owner).

41. Further, competition authorities, when they collect electronic evidence, should be able to retrieve the "technical entirety" of the evidence, meaning, for instance, the entire thread of an e-mail exchange and its attachments, although it may be decided that not all of it should be included in the investigation file.[23] This has been clarified by the European Commission in its revised Explanatory Note of 2015 where it stated that:

> *Each evidence item selected during the course of the inspection may be collected and on-site listed in its technical entirety (if e.g. only one attachment to an email is selected, then the final export will consist of the cover email, along with all attachments that belong to that particular message).*

42. Seizing whole hard-drives or servers for later examination of the documents and files contained in them, however, may raise privacy issues linked to the fact that the data may include personal information together with work information, or it may go beyond the scope of the investigation as defined in the competition order or the court warrant. This question is right at the core of the issue of the proportionality of the investigation.[24] Therefore, when this power is recognised, the rights of defence of the company must be protected by the competition authority also during the preliminary phases and should not be irreparably prejudiced.[25]

43. When the data needs to be examined at the competition authority's premises, to preserve the rights of defence of the company, and in particular the legal professional privilege and the protection of privacy, it may be important that some conditions are respected. Depending on the legal framework, these may, for instance, include: i) the sealing of the data carrier; ii) the deletion of all irrelevant data copied from the file;[26] iii) the provision of a list of the documents copied; or iv) the presence of lawyers at the opening of the seal and throughout the examination of the data at the competition authority's premises.[27]

44. Alongside or in alternative to these precautions, some in-built guarantees may be also included into the digital tools used for evidence gathering, for instance by ensuring that search software or algorithms would not go beyond the scope of the investigation as described in the authority order or court warrant.

Box 4. The procedure followed by the European Commission in *Nexans* France

By decision of April 2014, the European Commission sanctioned European, Japanese and South Korean producers of high and extra-high voltage power cables for participating in a market-sharing cartel.

The inspection was conducted by the European Commission over 4 days at the premises of Nexans France. During the inspection, the European Commission took copy-images of the hard drives of the computer of 3 employees and carried out keyword search on the basis of indexation. It sealed the office of a fourth employee who was not present at the premises of the company at the beginning of the investigation. Upon return of this fourth employee on the third day of the inspection, the European Commission discovered that some data had been deleted from his computer. The officials made copy-images of the hard drive of this fourth employee's computer, which they placed in sealed envelopes and brought to Brussels.

The European Commission then proceeded to the examination, always in the presence of Nexans' lawyers, opening and re-sealing the envelope every day for the duration of the examination. The relevant documents were printed and a copy and a list of those relevant documents was given to the company's lawyers.

The company appealed the decision. No infringement of the rights of defence was alleged, because the same procedural safeguards, such as the presence of the lawyers and the sealing of the rooms and envelopes, were taken for the examination of the digital documents at the Nexans' premises and at the Commission's premises. Nexans, however, argued that, *inter alia*, Article 20(2) of Regulation 1/2003 does not grant the Commission with the power to take copies of documents that had not been examined beforehand at the company's premises, nor to examine those documents later at the Commission's premises.

Under this provision, European Commission officials can access companies' premises, examine books and business records regardless of how they are stored and take copies or obtain extracts.

The General Court concluded that Article 20(2) of Regulation 1/2003 does not limit the power of the European Commission to make copies only of those documents that it has already reviewed.

The judgment of the General Court is under appeal before the Court of Justice. A similar issue is currently pending before the Court of Justice in the *Prysmian case.*

This issue has been addressed in the EU Member States by the entering into force of Article 6(1)(c) of the ECN+ Directive, which recognises the power for competition authorities to continue inspections at the premises of the national competition authorities or at other designated premises, and that will have to be transposed by the EU Member States by 4 February 2021.

Sources: General Court of the European Union, T-449/14, Nexans France and Nexans v Commission, 12 July 2018, ECLI:EU:T:2018:456, Appeal before the Court of Justice C-606/18 P and Court of Justice of the European Union, C-601/18 P, Prysmian and Prysmian Cavi e Sistemi v Commission, pending.

3.2. Access to personal electronic devices and data

45. A second issue potentially arising in investigations involving the gathering of evidence by means of digital tools concerns the interplay between the investigation powers and the right to privacy. It is generally considered that the protection of confidentiality and privacy does not raise significantly different challenges in relation to physical and digital evidences (OECD, 2018d, p. 5). One specific challenge, however, emerges in relation to the access to personal or semi-personal electronic devices and other data storage systems that may be held by employees at the premises of the company. With the diffusion of internet and of personal mobile phones, the number of companies allowing employees to use personal electronic devices for work purposes has increased.

46. This means that, in some cases, personal devices may contain evidence of an infringement or communications that are private or semi-private may be also used to perpetrate a violation of competition law.

47. In some jurisdictions, like France, the authority has the power to inspect personal electronic devices containing work-related information. In its revised Explanatory Note of 2015, the European Commission specifically stated that:

> *The Inspectors may search the IT-environment (e.g. servers, desktop computers, laptops, tablets and other mobile devices) and all storage media (e.g. CD-ROMs, DVDs, USB-keys, external hard disks, backup tapes, cloud services) of the undertaking. This applies also to private devices and media that are used for professional reasons (Bring Your Own Device - BYOD) when they are found on the premises.*[28]

48. A similar position is adopted in the 2019 draft Peruvian Inspection Guidelines, which also provide for the possibility that, during the inspection, the representatives or employees of the company may indicate the personal character of the inspected files or documents, to avoid, if appropriate after verification by the officials, their seizure.[29]

49. A decision adopted by the Spanish CNMC mentions that access to files, work-related or personal, cannot be prevented by the investigated company nor constitutes a violation of its rights of defence, when it may be necessary to preliminary determine the relevance of the examined documents for the investigation.[30] In other jurisdictions, like Colombia, recent case law did not seem to clarify whether this power to also access personal files for a preliminary examination may be exercised by the competition authority.[31]

50. When the legal framework does not specifically provide that these data can be copied or the case law did not clarify this issue, claims over privacy may be raised in court and slow down or prevent the full exercise of the power of investigation by the competition authority.

51. When a combination of private and work data is found, and no specific guidance is provided by the law or the jurisprudence, the approach to take for competition authorities may also vary depending on the way in which the information is copied.

52. If the digital copy is made from standalone data carriers, where it is possible to extract only the relevant information, the investigated company may identify the private data to avoid its copying or seizure. In case of disagreement concerning the nature of the information, procedures akin to the 'sealed envelope' procedure, where the information is seized but not examined by the authority until a formal decision is taken, may be adopted.

53. If the digital seizure is done by means of imaging, the separation of the relevant and the private data will not be possible, due to the nature of the procedure itself (OECD, 2013a, p. 13). One way to overcome this issue may be to invite the company representatives and the lawyers at the competition authority's premises to assist during the examination of the imaged data and to ask them, before starting the examination, to indicate the private data they wish to exclude from the analysis (ICN, 2014, p. 28).

54. The power of competition authorities to examine private or semi-private devices if they contain work related information may become increasingly more important also in light of the fact that instant messaging applications, like WhatsApp, Skype or MSN, more and more often feature among the preferred ways of communication by means of which an anticompetitive agreement is reached and maintained.[32]

55. In addition to the increasingly more promiscuous use of business and personal means of communication and data storage, brought by the internet revolution, a less stark divide between business and personal devices has been accentuated by the Covid-19 pandemic and the teleworking policies adopted companies throughout the world. In this changed world, the power of competition authorities to search and seize work-related information stored on personal devices is likely to become more and more crucial.

56. In the event of claims over the privacy of the data, it is important that they are carefully and swiftly assessed to determine their robustness, in order to avoid the risk that unlawful communications may be exchanged on personal devices exclusively to the purpose of avoiding enforcement and that they disrupt and lengthen the investigation. The assessment may be carried out, in some jurisdictions, by an official working on the case, but in other jurisdictions it may be done by an independent third party, such as competition authority's staff not involved in the case or judicial authority (ICN, 2014, p. 28).

Box 5. The delay of the investigation due to challenges on procedural issues: the Portuguese Banks case

In 2019, the Portuguese Competition Authority (AdC) fined 14 banks for an information exchange of sensitive commercial data over more than 10 years. The banks involved in the concerted practice were fined a total amount of EUR 225 million.

The investigation started with a leniency application and involved dawn raids in 25 locations. Pending the investigation, some of the investigated banks raised procedural challenges concerning, inter alia, the confidentiality of the information seized. The investigated banks lodged 26 appeals on procedural issues that led to 43 proceedings. Only 5 of the court decisions taken were favourable for the investigated bank, but the proceedings caused the suspension of the investigation for over 360 days.

Although it concerned the confidentiality of the information seized, this case shows the impact that (founded or unfounded) procedural challenges may have on the length of the investigation.

Source: Parr, Portuguese decision shows banks filed 26 court proceedings during probe, 10 January 2020, https://app.parr-global.com/intelligence/view/1926305.

3.3. Access to servers in a different location from the business premises

57. A third issue arises in connection to the location of digital information, because storage space, such as servers and cloud computing, is often separate from the physical location of the data entry point. Inspections, therefore, may require accessing data stored on servers or other storage systems located at other physical premises (such as at another address of the investigated companies or at the premises of a third party, either in the same or in a different jurisdiction) or online in no physical space (ICN, 2014, p. 29).

58. In relation to this issue, the ICN identifies two types of approaches. The first one, called the "access approach" is the one according to which any piece of information which is accessible, can be used or controlled from the premises of the company can be searched and seized by the competition authority. The location of the storage is irrelevant. As mentioned in the Introduction, the 2019 OECD Council Recommendation concerning Effective Action against Hard Core Cartels favours this approach when it refers to the power of competition authorities to *"[a]ccess electronic information that could help establish a cartel violation including electronic material that is stored remotely (e.g. on 'the cloud') […]*".[33]

59. The second approach, called the "location approach" is the one according to which, if the storage of the data is not at the premises of the company, and given that an inspection order only allows to enter the premises of the legal entity named in it, this alternative location needs to be covered by the authority's order or the judge warrant (ICN, 2014, pp. 28-29).

60. In this second case, it may be significantly more difficult for a competition authority to access the relevant evidence. First, it will have to determine the exact location of the servers at another company's location. This will not be possible for cloud computing systems storing data online. Second, the lapse of time required to access the alternative location, if discovered after the beginning of the inspection, may be exploited by the company to move, destroy or alter evidence (See Box 1).

61. In some jurisdictions, the access approach has been recognised by the law. For instance, Article 6(1)(b) of the ECN+ Directive, already mentioned above, provides for the power "*to examine the books and other records related to the business irrespective of the medium on which they are stored, and to have the right to access any information which is accessible to the entity subject to the inspection*." In other jurisdictions, it may still be controversial whether the access approach is followed.[34]

62. In cases where the competition authority does not follow the more favourable "access approach", other forms of co-operation along the lines of the G8 24/7 High Tech Crime Network, which provides points of contact in adhering countries to request immediate support in investigation involving electronic evidence, such as data preservation requests[35] or co-operation with agencies outside the relevant jurisdiction may also prove necessary. The ICN noted that, "*In these cases the competition agencies use the possibility of mutual legal assistance treaties (MLATs) or agreements to gather the digital information*" (ICN, 2014, p. 29).

63. It is, however, important to underline that companies may strategically select as the 'hub' of a cross-border cartel a jurisdiction where it is harder for a competition authority to swiftly access evidence in an investigation, thus 'forum shopping' for procedural guarantees and weaker investigation powers (Scordamaglia-Tousis, 2014, p. 196). This makes the convergence on investigative powers and due process across countries extremely important.

Box 6. Open Issues

1. What are the best ways to ensure that a continued inspection procedure is conducted in full respect of due process?
2. In a world where teleworking has become the norm due to Covid-19 distancing measures, should personal electronic devices be allowed to be searched at all times? How can a competition authority strike the right balance between ensuring a thorough analysis of the relevant evidence and protecting privacy?
3. How do competition authorities ensure that the rights of defence of the company are observed in digital evidence gathering in cartel investigations?
4. What are the strategies adopted by competition authorities to overcome difficulties in accessing servers or information stored in digital cloud systems? What are the best ways to prevent destruction or alteration of evidence when this takes time?
5. Can international co-operation be used to stimulate convergence on investigative powers and due process across countries?

4. Building capacity for digital evidence gathering in cartel investigations

64. Digital evidence gathering requires a considerable investment for specific expertise (e.g. digital forensics, data analysis, artificial intelligence), tools (e.g. equipment, software) and infrastructure (e.g. rooms dedicated to forensics) that must be updated frequently according to the rapidly changing technology. Building and maintaining digital evidence gathering capacity is more costly than traditional evidence gathering capacity and calls for the support and understanding of the management.

65. At the same time, many competition authorities are facing budgetary freezes or restrictions. In fact, as highlighted by the OECD Competition Trends 2020, average budgets of competition authorities have decreased in real terms by approximately 5% between 2015 and 2018. (OECD, 2020b, p. 11) It would seem that this trend is unlikely to be overturned in the near future in view of the governments' budget constraint caused by the Covid-19 outbreak.

66. Consequently, it will be all the more important for competition authorities to continue to make an efficient use of their limited resources when designing their internal structure for digital evidence gathering. Moreover, external co-operation with other agencies should help to realize further resource efficiency in the organisation of digital evidence gathering.

4.1. Internal organisation for digital evidence gathering

67. A number of competition authorities have invested important resources to the development of digital evidence gathering capability. For instance, the Brazilian competition authority (CADE) started in 2014 the development of data mining instruments and economic filters to support its staff involved in the investigations and case handlers [see Brain (Cérebro) Project in Box 7]. The Mexican competition authority (COFECE) has also been investing resources in the training of forensic experts and investigators as well as hardware and software. (OECD, 2018c, p. 7) While these capacity-building actions are undeniably fruitful, securing the budget covering the high costs associated with these

actions could be a significant challenge for competition authorities. In this respect, ICN recommends to have a dedicated annual or multi-annual budget for digital evidence gathering. (ICN, 2014, p. 14)

68. The budget, which ultimately determines available resources of authorities, will drive how the digital evidence gathering capability is organised within the authority. Certain competition authorities have a permanent forensic IT unit for digital evidence gathering (e.g. EU (OECD, 2018d, p. 4), Portugal (OECD, 2018e, p. 15) or Korea (OECD, 2018f, p. 5)). These units, composed of digital forensic experts who work closely with agencies' officials and internal IT experts in the conduct of digital evidence gathering (and possibly in data analysis at a later stage), have reportedly provided significant added value to the digital evidence gathering.[36]

69. Depending on the circumstances of the case, several authorities have engaged outside IT forensic experts who work closely with the officials and internal IT experts of the authority (e.g. South Africa (OECD, 2018g, p. 2) or Australia (OECD, 2018h, p. 3)). As pointed out by ICN, such outsourcing may require a confidentiality agreement in order to provide appropriate safeguard for the confidential information that is made available to outside IT forensic experts. (ICN, 2014, p. 14) Another challenge seems to concern how to integrate outside experts well in the investigation team to maximize the profit of having IT specialists in the team. Outside experts could also be costly depending on the service provided. In this respect, ICN recommends to maintain a minimum internal IT capability, even in case where the outsourcing is used, in order to ensure that the appropriate service is provided at a reasonable price level. (ICN, 2014, p. 14) Minimum IT knowledge of the authorities' officials as well as minimum competition law knowledge of outside IT experts should also facilitate the swift integration of various expertise in the investigation team.

70. Irrespective of the design of internal capability for digital evidence gathering, it is indispensable to ensure that persons conducting digital evidence gathering are appropriately trained for that purpose. This could be accomplished by developing the skills of existing staffs or hiring experts from outside. Skills for digital evidence gathering encompass a number of specialised areas. They include for instance digital forensics which applies scientific techniques for identifying, preserving, recovering and analysing the digital information and presenting facts and opinions about it. (OECD, 2018a, p. 4) Other emerging technologies, such as artificial intelligence, internet of things, bid data and blockchain, should also be useful for the detection of cases requiring a thorough technical and economic understanding of companies' behaviour with regard to data and algorithms (see Box 7). As the UK Competition and Markets Authority rightfully highlighted, the power of algorithms can also be used by enforcement agencies to better enable them to interrogate large datasets to assess impacts on competition. (OECD, 2017, p. 12) Furthermore, persons conducting digital evidence gathering may need to be trained of the relevant legal standards and challenges described above in order to ensure that the procedure is conducted within the boundaries of the relevant legal framework.

Box 7. Cartel Screening: a Pro-active Cartel Detecting Tool

Cartel screening tools have become important pro-active instruments to mitigate the dependency on reactive tools such as whistle- blowing or leniency applicants. The growing availability of data and computing power provides competition authorities efficient ways of detecting atypical signs or suspicious behaviour associated with collusion.

Cartel screening certainly serves as an effective tool for cartel detection, but also it generates an additional deterrence effect by encouraging firms to submit leniency applications, to sign cease and desist agreements and to report anticompetitive conducts to competition authorities.

Screening refers to a detection methodology designed to help competition authorities decide which markets or industries are more likely to be prone to cartel behaviour, and in some cases they can also flag to them possible cartel behaviour that would deserve closer scrutiny. (OECD, 2013, p. 5) In other words, an industry that is picked up by a screen is one that warrants not prosecution but rather a more intense investigation which directly contrasts collusion and competition as competing explanations of market behaviour. Screening is then the first phase of a multi-stage process which may or may not end with prosecution. (Harrington, 2007, p. 2)

There is a growing literature on cartel detection, which can roughly be divided into two strands. (Imhof, Karagök and Rutz, 2018, p. 237; OECD, 2013, p. 5) One approach, commonly referred to as "structural screening", is based on what economic theory and empirical research tell us about the relationship between market characteristics and the likelihood of collusion occurring in markets, essentially by identifying certain structural features of products or market which facilitate collusion. This approach may enable a competition authority to screen any number of markets or industries in order to flag those markets where a cartel is more likely to occur.

The second approach, based on "behavioural screening", is used for indicating whether a specific market was actually affected by collusion. Of course, direct evidence of cartelisation is not easily observable and is hard to uncover. However, economic theory and analysis of data on observed cartels has identified various types of observable traces that the creation, life, and break-up of a cartel are likely to leave behind. These trails are what behavioural screens are designed to detect.

These two approaches do not exclude each other. On the contrary, they are usually viewed as complementary, so that if the structural screening gives positive results, authorities can proceed with a more targeted review based on firms' behaviour and their consistency with a competitive process.

Screening is a resource and data intensive method. Sufficient, relevant and accurate information and data are necessary for all stages of screen implementation, from screen design, to the implementation of the screen, up to the interpretation of its results. Accessing this information is a key issue in any empirical methodology. Screens may also be quite sensitive to the quantity and quality of the data used as input. For example, running a price-variance screen on aggregated data (e.g. average yearly or monthly prices) found in market studies may lead to completely different results from running the same screen on disaggregated data (e.g. daily quotes).

Cartel screening methods have been widely used by several competition authorities, including following:

Brazil's "Cérebro (Brain)" project

The Administrative Council for Economic Defense (CADE) has developed a screening project called Cérebro (the "Brain") since 2014. Cérebro is a platform that allows the integration of large public procurement databases by applying data mining tools and economic filters capable of identifying and measuring the probability of cartels occurring in public bids.

Cerebro's data mining tools allow for the automation of the analyses formerly conducted by investigators and case handlers. The objective is both the identification of evidence of cartels in public bids, such as suspicious, implausible facts or behavioural patterns, and the provision of relevant information for the investigation of the cases. The economic filters in the platform are based on specialist literature and econometrics. They seek to provide generalised evidence of the existence of cartels based on data related to prices, costs, profit margins, market share, etc. Through the identification of firms' behaviour as described in academic articles, CADE derived mathematical models as statistical tests for general use in a kind of reverse engineering process.

Some investigations have been started as a result of the Cérebro tool. It is still early days and the courts are considering whether the information it provides is sufficient to meet the threshold for the authorisation a warrant for a dawn raid.

Colombia's ALCO program

The Colombian competition authority (SIC) has been participating in a project to develop a procurement data tracking software program ("ALCO") since 2013. The program is designed to help identify patterns of conduct by bidders that suggest collusive behaviour and flag it to SIC.

Chile

Chile's Competition Authority (FNE) uses procurement data to perform screening exercises. FNE and the central purchasing body ChileCompra have a co-operation agreement that allows the FNE to monitor tenders through ChileCompra's database.

Mexico

In 2015, Mexico's Competition Authority (COFECE) created a market-intelligence unit inside its Investigation Authority (IA), which is fully dedicated to monitoring markets and screening market data to gather sufficient evidence to initiate antitrust investigations. Over the period 2016-2019, approximately 20% of investigations were initiated through findings of the market-intelligence unit.

Peru

The Peruvian competition authority (INDECOPI) developed indicators for the detection of bid rigging in the procurement of liquid fuel between 2007 and 2013, based on economic criteria and data provided by the Peruvian Public Procurement Supervisory Body (OSCE).

Korea's Bid Rigging Indicator Analysis System (BRIAS)

In 2006, the Korean Fair Trade Commission (KFTC) developed the Bid Rigging Indicator Analysis System ("BRIAS") to help detect bid rigging. BRIAS is an automatic quantitative analysis IT system which analyses large amounts of online public procurement data and, based on indicators incorporated in it, quantifies the likelihood of bid rigging.

BRIAS collects online public procurement data concerning large-scale contracts awarded by central and local administrations within 30 days of the contract award. Then, the system analyses the data and generates scores on the likelihood of bid rigging by assessing factors like tender method, number of bidders, number of successful bids, number of failed bids, bid prices above the estimated price, and price of winning bidder. Each of these factors is assigned a weighted value and all values are then added up. For instance, higher rates of successful bids and lower number of participating companies are indicative of a possibility of collusion. All bids are also screened according to search criteria like the name of the winner candidate, or bids with similar score.

A total of 16 public procurement agencies were participating to BRIAS, including central administrative agencies and state-owned companies. Between 2015 and 2019, BRIAS flagged more than 5,600 cases for further analysis, and the KFTC initiated 783 investigations.

Source: OECD (2020; 2019; 2016); KFTC

4.2. External co-operation for digital evidence gathering

71. In addition to the efficient internal organisation, external co-operation should further help to reinforce competition authorities' digital evidence gathering capability. Co-operation may take place in a multiplicity of forms, including bilateral/multilateral co-operation agreements, memoranda of understanding, mutual legal assistance treaties or *ad hoc* co-operation.[37] It could be envisaged with other national agencies (such as financial or telecom regulators) as well as other competition authorities.

4.2.1. Co-operation with other national agencies

72. Digital evidence gathering has been developed not only for the purposes of competition investigations but also for the detection of other illegal conduct, such as manipulations of stock and commodities prices and indices, revenues management, stock options back-dating, insider trading, and tax evasion. Many public agencies, such as financial regulatory authorities, procurement agencies and energy or telecom regulators, also make use of digital tools in their enforcement and monitoring responsibilities. Co-operation with these agencies therefore has great potential for synergies for digital evidence gathering.

73. Against this background, several competition authorities have put in place a co-operation framework with other public agencies for the retrieval, copying and analysis of digital evidence. For example, the Chili competition authority (FNE) entered into a co-operation agreement with the government procurement body (Dirección de Compras y Contratación Pública "Chilecompra") that allows the FNE to monitor the tenders through the database available in Chilecompra's technology sources. (OECD, 2013, p. 99, see Box 7 for other examples) Co-operation could also relate to joint seminars, trainings or workshops as well as sharing of knowledge and experience for digital evidence gathering. For example, the French General Directorate for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF), which developed expertise in the field of digital inspections since early 2000, shared its knowledge with the French competition authority created in 2008. (EC, 2016, p. 6) This type of co-operation seems relatively easier to implement and should thus be encouraged since it does not require formal agreements or memorandum of understanding.

Box 8. ICN recommendation on co-operation with other public agencies

With respect to the co-operation with other public agencies for digital evidence gathering, ICN recommends to describe the scope and nature of co-operation with other public agencies in a protocol that covers the responsibilities and procedures of cooperating agencies during the digital evidence process.

According to ICN, the protocol should cover the responsibilities and procedures of the co-operation agencies during the digital evidence gathering process. Furthermore, they should outline the handling and exchange of retrieved data.

ICN also provides specific points that may be usefully reflected in such a co-operation protocol:

- Hours that the other agency will provide and how they will be calculated (overtime on a mission; specific periods and so on); maximum time on mission; training for team;
- Material that will be made available: hardware, software, supporting material;
- Names and/or qualifications of the staff that will provide the support;
- Minimum time period that support staff will be informed before an intervention;
- Price of the service/contract; and
- Duration of contract and review modalities.

Source: ICN, 2014, p. 14.

4.2.2. Co-operation with other competition authorities

74. International co-operation should further help to efficiently build digital evidence gathering capability. Co-operation could take place for instance in the form of joint capacity-building activities. Several competition authorities have indeed established a co-operation scheme in order to further boost their digital evidence gathering capability. For instance, within the framework of the European Competition Network (ECN), a working group on forensic IT was established in 2010 to serve as a forum for the exchange of information and best practices on technical and legal issues surrounding the use of forensic IT tools.[38] Taking into account the development and importance of artificial intelligence in cartel investigations, the name of the working group has recently been changed from ECN Forensic IT working group to the ECN DIAI (Digital Investigations and Artificial Intelligence) working group.[39]

75. International co-operation could also be extended into more substantive aspects of digital evidence gathering. This is particularly relevant in terms of access to digital evidence located abroad and sharing of digital evidence between authorities (within the boundaries of the relevant legal framework). However, as highlighted in the context of previous OECD work, while international co-operation in cartel cases has reached unprecedented levels in recent years, a number of obstacles to effective co-operation would appear to remain. These include the inability to share confidential information, the difficulties of gathering evidence located outside of the jurisdiction concerned and the undertaking of joint digital inspections.

Box 9. Open Issues

- How can competition authorities secure sufficient budget to build-up digital evidence gathering capability?
- How can competition authorities design their internal digital evidence gathering capability? Should they focus on developing the skills of existing staffs or hiring experts from outside?
- What are the best practices for a better integration of outside IT forensic experts in the investigation team?
- What are the key skills required for officials and forensic experts for the digital evidence gathering? In this connection, what would be the ideal profile of the staff working on it? Competition experts with forensic skills or forensic experts with competition law training?
- How can competition authorities ensure effectiveness of co-operation with other public regulators and competition authorities for the purpose of the digital evidence gathering? What form of co-operation would be desirable?
- What are the obstacles to international co-operation for digital evidence gathering? What measures could be taken to tackle with them?

5. Conclusions

76. This Issues Paper briefly sketched some of the legal and practical challenges that may be encountered by competition authorities in connection with the gathering of digital evidence in cartel investigations. Ever evolving tools for the gathering of digital evidence are increasingly being developed, magnifying the powers of competition authorities to collect high volumes of data and information in a swift manner.

77. The importance of these tools is also likely to increase in connection with the current Covid-19 pandemic, which, due to lockdown measures and the working from home policies adopted by many companies, changed the way in which competition authorities and businesses operate.

78. The new opportunities may, however, on the one hand, raise a few legal challenges linked to their extent and outreach, which may clash with the right of defence of the company or conflict with the right to privacy. A careful balance should be struck to enable the competition authority to fully exercise its powers, without unnecessarily intruding into the business operation and the personal lives of the employees.

79. On the other hand, the adoption of digital tools may require some adaptation and internal coordination of budgetary and human resources and external co-operation with governmental bodies or other authorities to ensure that they are fully exploited. This may require significant resources, which call for adequate planning and design of the most cost-effective strategies that are suitable for any specific competition authority depending on the environment in which it deploys its activity.

80. The various challenges and the need to maximise the use of the opportunities offered by digitalisation also show the importance of international co-operation between competition authorities to exchange experiences and best practices on the adoption and use of digital tools in a way that minimises the risk of challenges and that it is most suitable and efficient.

End Notes

[1] OECD (2020), Government at a Glance: Latin America and the Caribbean 2020, OECD Publishing, Paris, https://doi.org/10.1787/13130fbb-en, p. 12.

[2] The Economist, Rigging the Bids Nov 19, 2016, https://www.economist.com/europe/2016/11/19/rigging-the-bids.

[3] OECD (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] OECD (2016), Promoting effective competition in public procurement, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/LACF(2016)31&docLanguage=En.

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

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

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

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

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

[10] A forensic imaging is a process copying all data contained on a storage medium, including the unallocated space. It is also called "mirroring" due to the fact that a mirror image of the content of the storage medium is created.

[11] In practice, various software programs are used for digital forensics, among which *EnCase* and *Nuix* are the most popular programs used by various competition authorities. However, not every authority uses forensic tools, and in those cases, digital sources of evidence are copied through inbuilt search tools and deleted data is retrieved and copied from "recycle bins" or backup servers.

[12] Live forensics consists of seizing or analysing system information, memory contents and/or contents of data carriers from live systems (i.e. systems that are on/running). This extracts information from live memory (i.e. information which is lost when the computer devices or systems are turned off/powered down)." (ICN, 2014, p. 6)

[13] Chain of evidence is record of seizure, analysis and other processing of the digital evidence, which proves the evidence is extracted from the seized digital information without doubt. In most jurisdictions, it is necessary to have a valid record of the authenticity of the digital evidence, or proof that the digital evidence is unequivocally identical to the acquired digital information, in order for the digital evidence to be legally admissible. Chain of custody is the record of the custodial history of the evidence. In most jurisdictions, having a valid record of the chain of custody, or describing who has had physical possession, and why and where they had physical possession, is required for legal admissibility of the evidence in court. (ICN, 2014, p. 5)

[14] A hash value is a unique numeric value that identifies data like a digital finger print. It is produced by mathematical algorithms. Data cannot be changed without changing the corresponding hash value. If somebody changes afterwards one single dot in the data container, this will change the hash value. It is therefore a guarantee that, as long as there is the same hash value, the container contains identical data.

[15] The ECN (2013, p. 4) recommends a continued inspection procedure as an effective way of digital evidence gathering. This procedure grants more time to further search the data and better understand the case so increases the possibility to detect relevant evidence in the often voluminous digital case file. In addition, this procedure minimises the disruption of the undertaking's operations. However, it is also argued that copying and taking away a huge amount

of data for review/sifting potentially risk the violation of basic rights such as privacy or violations of legal privilege of firms under inspection (OECD, 2018a, p. 6).

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

[17] To give just a few examples, a court warrant is normally requested for a dawn raid in Australia, Austria, Chile, France, Germany, and Romania.

[18] Court of Justice of the European Union, C-37/13 P, Nexans SA and Nexans France Sas v European Commission, 25 June 2014, ECLI:EU:C:2014:2030, para. 33.

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

[20] Opinion of Advocate-General Kokott in C-606/18 P, Nexans France and Nexans v European Commission, 12 March 2020, ECLI:EU:C:2020:207, para. 77.

[21] Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, OJ L 11, 14 January 2019, p. 3–33.

[22] Opinion of Advocate-General Kokott in C-606/18 P, Nexans France and Nexans v European Commission, 12 March 2020, ECLI:EU:C:2020:207, para. 59.

[23] European Commission, Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003, 11 September 2015, para. 16.

[24] The current OECD Draft Recommendation of the Council on Transparency and Procedural Fairness in Competition Law Enforcement of 28 May 2020, DAF/COMP/WP3/WD(2020)23, recommends "applying appropriate internal competition authority checks and balances for procedural steps in order to ensure lawfulness, proportionality and consistency".

[25] See, on this point, Court of Justice of the European Union, C-46/87 and 227/88, Hoechst AG v Commission, 21 September 1989, ECLI:EU:C:1989:337, para. 15; Court of Justice of the European Union, C-204/00 P, C-205/00 P, C-211/00 P, C-213/00 P, C-217/00 P and C-219/00 P, Aalborg Portland and Others v Commission, 7 January 2004, ECLI:EU:C:2004:6, para. 63; General Court, T-135/09, Nexans France and Nexans v Commission, 14 November 2012, ECLI:EU:T:2012:596, para. 41.

[26] Opinion of Advocate-General Kokott in C-606/18 P, Nexans France and Nexans v European Commission, 12 March 2020, ECLI:EU:C:2020:207, para. 62.

[27] Opinion of Advocate-General Kokott in C-606/18 P, Nexans France and Nexans v European Commission, 12 March 2020, ECLI:EU:C:2020:207, paras. 82-83.

[28] European Commission, Explanatory note on Commission inspections pursuant to Article 20(4) of Council Regulation No 1/2003, 11 September 2015, para. 10.

[29] Indecopi, Proyecto de Lineamientos de Visitas de Inspeccíon, October 2019, https://www.indecopi.gob.pe/documents/51771/2962929/Lineamientos+de+Visitas+de+Inspecci%C3%B3n/, pp. 34-35.

[30] CNMC, Decision R/0148/13, Renault, 23 September 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, June 2020, https://www.competitionpolicyinternational.com/wp-content/uploads/2020/06/Latin-America-Column-June-2020-Full.pdf.

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

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

[34] See, for instance, Canada, where "Bureau investigators have downloaded data stored outside Canada in the course of searches of computer systems located in Canada, although there continues to be some controversy as to the precise limits of the authority granted by a warrant authorising a search of computer systems in a cross-border context.", https://www.lexology.com/gtdt/tool/workareas/report/617528c4-0e23-4678-a460-9333ed458dc0.

[35] For further details, see http://www.oas.org/juridico/english/cyb20_network_en.pdf, and http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf

[36] For instance, in some cases, the forensic IT team enabled the investigators to restore emails that were intentionally deleted by employees of the company investigated (OECD, 2018d, p. 4 (EU) and OECD, 2018f, p. 5 (Korea)).

[37] For further information, see OECD roundtable on "Improving International Co-operation in Cartel Investigations". http://www.oecd.org/daf/competition/ImprovingInternationalCooperationInCartelInvestigations2012.pdf.

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

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

References

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.