

Unclassified

English - Or. English

22 September 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

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

- Contribution from Mexico -

28-29 September 2020, virtual Zoom meeting

The attached document from Mexico is circulated to the Latin American and Caribbean Competition Forum FOR DISCUSSION under Session I at its forthcoming meeting to be held on 28-29 September 2020, via a virtual Zoom meeting.

Ms. Lynn Robertson, Manager Africa/MENA, LACCF ; Competition Expert - Lynn.Robertson@oecd.org.

JT03465637

Session 1: Digital Evidence Gathering in Cartel Investigations

– Contribution from Mexico –*

1. Powers to gather evidence in digital format

1. The Federal Economic Competition Commission (the Commission) has an institutional model that separates its investigation and decision-making functions. In this sense, the institution has an Investigative Authority (IA) and a Plenary that makes decisions subject to deliberation.¹

2. The IA is responsible for investigating: i) monopolies, both absolute² and relative,³ and unlawful concentrations;⁴ ii) barriers to competition and essential inputs that can generate anti-competitive effects;⁵ and iii) the existence of effective competition.⁶ The investigations of the IA determine if there is evidence of anti-competitive conduct or conditions in a market. If this is the case, it issues an opinion of probable or preliminary responsibility, which it passes to the Technical Secretariat⁷ to initiate ensuing trial proceedings. At this stage, the economic operators concerned can make declarations and provide evidence relating to the presumptive charges against them. Once these declarations have been made, the evidence has been set out and the corresponding pleas have been presented, the plenary session of the Commission may make a ruling in conformity with the law.

* This contribution was prepared by the Mexican Federal Economic Competition Commission.

¹ The Plenary is the governing body of the Commission, entrusted with the task of resolving, with full independence and autonomy, subject to deliberation and by majority voting, the cases and matters it is constitutionally mandated to deal with. It comprises seven Commissioners, including the Chair. They are chosen by an evaluation committee comprising the heads of the Bank of Mexico, the National Institute for Assessment of Education and the National Institute of Statistics and Geography, which examines and determines the technical capabilities of potential Commissioners. Based on these results, they are selected by the Federal Executive and ratified by the Senate of the Republic.

² Article 53 of the LFCE, also known as cartels.

³ Articles 54-56 of the LFCE, which may be vertical restrictions, abuse of dominant position.

⁴ Article 62 of the LFCE.

⁵ Article 94 of the LFCE.

⁶ Article 96 of the LFCE.

⁷ The Technical Secretariat of the Commission is empowered to conduct proceedings in the form of a trial in cases of monopolistic practices and unlawful concentrations, as well as the second stage of the procedures for determining barriers to competition, essential inputs and the existence of effective, competitive market conditions. It is also responsible for authenticating votes, taking minutes and preparing the stenographic versions of Plenary meetings. Likewise, it is responsible for substantiating the analyses of concentration notified by economic operators; issuing opinions on the terms of tenders, concessions or permits and their participants; issuing opinions and recommending actions to promote competition in respect of programmes, policies, provisions or regulatory acts; conducting economic studies on conditions of competition in markets. The directorate-generals for Concentrations, Legal Affairs and Market Studies are attached to this Secretariat.

3. To carry out the above-mentioned investigations effectively, the Federal Law on Economic Competition (LFCE) grants investigative powers to IAs in all cases, including inspections, requesting information from economic operators or authorities, and holding hearings. Digital evidence on cartels is normally gathered during inspections. It is also gathered in response to information requests (there are cases where it is explicitly requested that these requests be answered in digital form, and others where it is presented in this format for ease of handling).

4. Digital information is often obtained from both monitoring and screening,⁸ as well as from inspections and responses to information requests. It can subsequently serve as evidence of a cartel to impute probable liability to natural and legal persons. It can also be used as evidence in proceedings in the form of a trial, as well as in the courts, in cases where the Commission's decision is appealed.

2. Digital evidence obtained from investigative tools

5. During inspections, digital data are usually gathered by making a forensic copy of electronic devices in whole or in part (e.g. only the institutional e-mail account or folders selected by the inspection leader). Once the data have been compiled on site, it is processed at the Commission forensic laboratory and the information is reviewed to identify whether it includes communications protected by lawyer–client confidentiality, which should be excluded from the information bank for investigator consultation.

6. To protect the defence rights of economic operators that form part of the investigation, the “Regulatory Provisions of the Federal Economic Competition Commission, for the classification of information derived from legal advice provided by economic operators”⁹ require the Commission to extract such information by virtue of the office held, if the economic operators do not submit a request for qualification.¹⁰ If this type of information exists, the file shall be excluded from the dossier, which shall be recorded in a circumstantial record.¹¹

7. To analyse and process the data obtained from an inspection, the investigative departments are supported by the capacities and tools of the Directorate-General for Market Intelligence (DGIntM), also attached to the IA. The DGIntM is responsible for assisting the directorates of investigations (DIs) to conduct forensic information analysis, process digital data for use by DIs, carry out market monitoring and screening of information to issue market reports for opening investigations, and provide strategic information to help identify lines of investigation.¹²

8. In addition, the DGIntM carries out intelligence work to detect and verify addresses, a key element of effective inspections, since if part of the address is incorrect, the subject of the inspection may refuse the IA entry on grounds of producing an inspection order with incorrect information. In addition to using internal tools, DGIntM and the

⁸ Screening refers to the use of digital tools to detect structures and behaviours that indicate the likely existence of cartels.

⁹ Available from the following link: <https://www.cofece.mx/wp-content/uploads/2019/09/DOF-30septiembre2019-01.pdf>

¹⁰ Article 5 of the Regulatory Provisions.

¹¹ Article 12 (II) of the Regulatory Provisions.

¹² Article 31 of the LFCE.

Directorate-General for Investigation of Absolute Monopoly Practices (DGIPMA) have both received specialist training in this area.

9. Furthermore, many responses to information requests are in digital format, either because the economic operator considers this format more manageable or because the information request states that certain answers must be given to the authority in a specific format and in compliance with certain specifications. In this respect, requests set a deadline for the response and provide detailed instructions for each section indicating how the requested information should be provided. For example, economic agents are usually asked to provide historical price data, customers, fixed costs, variable costs, etc. in Excel (.xlsx) format with a table indicating each item per year and a separate sheet for each question in the information request.

10. To ensure information obtained from inspections and information requests is useful, filters are put in place, databases are created and data are analysed to identify the files or data that could be used in the investigation. The investigation teams and the DGIntM IT specialists work jointly to achieve this.

11. It is also essential for IAs to protect digital information and data obtained through inspections and information requests. In the first case, forensic laboratory tools are used to ensure the protection of personal and private information obtained. This involves creating digital locks so that only information related to the inspection order (i.e. the market under investigation) can be accessed.

12. There are also internal protocols that classify all information in a file as reserved or confidential. Reserved information can only be reviewed by those in charge of the investigation, while confidential information is separated from the main dossier and can only be consulted by the Director-General of Absolute Monopoly Practices and designated officials. For example, information considered confidential may include business strategies, customer lists, personal data and industrial secrets.

3. Digital evidence gathered from the Intelligence Unit

3.1. The Directorate-General for Market Intelligence

13. The DGIntM was created in 2014 to fulfil the powers granted to the Commission as a result of the constitutional reform that year. It began by providing the capacity and resources needed to gather digital information when conducting inspections. The department then became more specialised, until the creation of the forensic and intelligence unit it manages today.

14. This unit develops and employs digital tools to detect structures and behaviours that signal the likely existence of cartels. This procedure is known as screening. To do this effectively, there is a specialised team, half of which focuses on screening and economic analysis, while the other half performs forensic and operational intelligence functions.

15. This area comprises the most diverse profiles in the IA (e.g. specialists in security, mathematics and psychology) and staff with the highest levels of graduate studies in the IA (approximately half the team has at least a master's degree or higher studies).

3.2. Data collection, processing and analysis tools

16. A number of tools have been developed or are used for this task: cluster computing tools for big data (e.g. Apache Spark); automated tools for extracting information from Internet sites (web scraping); statistical, interdisciplinary and graphical analysis tools using specialised computer programmes; parallel computing; cloud computing; and artificial intelligence algorithms (e.g. machine learning).

17. These tools facilitate or allow big-data analysis of market structures and behaviours that involve data with high levels of volume, variety, speed and value. The implementation of these tools has made certain cartel detection activities performed by the authority more efficient. They have also streamlined processes and enabled the analysis of anti-competitive behaviours.

3.3. Screening

18. It is important to note that all these tools are used to extract, process and analyse information from different markets, whose data can be obtained through digital media (e.g. government or private electronic sources) or those whose business models are fully or partially integrated into e-commerce channels.

19. These tools are specifically used to detect cartels in bidding markets, as this is a sector of the economy that the Commission has prioritised in its Strategic Plan 2018–2021.¹³ Consequently, screening procedures have served to build up indirect economic evidence using automated and semi-automated tools to detect suspicious patterns, such as stability in time series, breakdowns not associated with supply and/or demand conditions, absolute and/or relative differences between tenders, inconsistencies in recruitment cycles and trends in input prices.

20. A key element in public procurement processes is the central public database, Compranet, which publishes data on tenders and their results and which facilitates data gathering and processing. In this regard, the use of screening has been fundamental to the Commission, given that, on average, 25% of cartel cases opened each year involve some sort of data processing of this type.

21. To carry out screening procedures, data processing has been automated to contrast the average and variance of price series, making it easier to identify possible collusive patterns. For example, screening algorithms have been developed for public procurement databases (Compranet). The specialist data team also develops techniques and/or software to digitise information taken from the main sources consulted. This simplifies data analysis and enables the use of tools for information management through filters, tables, navigation resources, etc.

22. Screening is mainly used to detect collusion in regulated sectors and digital markets but also for public procurement. In contrast, market studies are used to detect anti-competitive conditions, such as the abuse of dominant positions and barriers to competition.

¹³ The full document is available at the following link.

4. Challenges gathering and processing digital evidence

23. The IA has faced a number of challenges gathering digital information prior to and during investigations. As in many jurisdictions, one of the main challenges is the availability and quality of information. In the case of Mexico, public procurement databases do not always capture information for the whole procurement process (from market studies to the evaluation of bids), which provides an isolated view of the results of tenders. There are also no centralised data governance frameworks in the country, resulting in inconsistencies in how information is recorded in the centralised public procurement database. Moreover, under the current structure, data on whether participants engage in subcontracting services or products is not made public, which makes it difficult to detect potential cartels.

24. Another significant challenge is the high level of investment required to adapt IT infrastructure (mainly for storage and processing for big data). At present, the most efficient and cost-effective solutions are based on the cloud.

25. Regarding forensic issues, the main challenge is copying digital devices during inspections. A key element is the forensic hardware purchased for copying, which has a direct impact on the copying capacity of the equipment and the speed at which the task is performed. In addition to the above, these tools require the most frequent upgrades, considering the speed at which the technology evolves. This has made it possible to optimise these processes significantly (reducing copying times by almost a third compared to the previous technology).

26. Another challenge in securing digital evidence during inspections is related to communications protected by lawyer–client confidentiality. There is a legal precedent for this, which recognised the protection of these communications for the first time in a competition case in Mexico. Derived from a petition pertaining to constitutional protections, which was granted to the complainant, information from an economic operator that the judicial body deemed to have been based on legal advice and thus could not be used as evidence by the Commission had to be removed from a hard drive.

5. Commission measures to address the challenges for obtaining digital evidence

27. In September 2019, the Commission established the Regulatory Provisions for the classification of information from legal advice provided to economic operators, which establish a specific procedure for handling communications protected by lawyer–client confidentiality. One paragraph of those provisions concerns the technical procedure for the exclusion of digital information.¹⁴

28. The qualification procedure is conducted by a Qualifier Committee consisting of three people from departments other than the DI in charge of the dossier. During confidential sessions, the Committee determines whether the information constitutes communication arising from legal advice. If the information is determined to be protected, its exclusion is ordered. For digital information, the DGIntM is responsible for deleting the file in question and must issue a record of the deletion.

¹⁴ Article 11, paragraph II.

29. Once the exclusion is ordered, forensic personnel conduct and document the technical procedure. The result of this technical procedure is that the digital information classed as confidential cannot be viewed in the analysis of the forensic images. This ensures the integrity of the image acquired during the inspection, avoiding alteration while ensuring compliance with the Committee resolution.

30. In addition, the DGIntM has internal procedures and standards to guarantee the rights of data defence and protection for economic operators recorded in an investigation dossier. There are mechanisms and measures to safeguard digital information, including those mentioned below.

31. *Copies of storage media acquired during inspections:* Economic operators subject to inspection may request copies of the storage media gathered in the inspection procedure for any analysis they consider relevant and, where applicable, for preparing the corresponding defence. To that end, providing an accurate copy (forensic image) of the media gathered by the Commission is key. Any information that comes from the storage media and may be used as evidence can be verified by the economic operator. Only economic operators subject to inspections can request copies of the media gathered. They are also given a copy of the inspection report and its annexes to ensure they have full knowledge of all the information available to the Authority.

32. *Protection measures for storage media:* The IA employs protection measures for storage media gathered during inspections. To this end, the inspection implements documentary measures, such as custody, traceability and control records, which function as custody chains. Physical measures are also implemented, such as packaging in sealed anti-static bags with security labels.

33. At the end of the inspection, the storage media are transferred by forensic technical personnel to the Commission and deposited in a security perimeter with restricted access controlled by physical and logical security systems. The storage media is held under protection.

34. All consultations of digital information take place in a forensic laboratory specifically designed for such analysis, with controlled access and restrictions on the entry of external electronic media.

35. Digital information on economic operators may only be consulted by Commission staff with the corresponding authority and powers. The mechanisms in force make it possible to accurately track all movements and access to the storage media available to the Authority.

36. *Availability of digital information used as evidence in the preparation of dossiers:* In the preparation of dossiers, specific versions are generated with extracts of the digital information used to file charges against economic operators for their conduct. This information is made available to the relevant economic operator to protect its right to defence.

37. Finally, it is important to mention that co-operation has been fundamental for the implementation, development and professionalisation of forensic activities. For example, since its implementation, the Commission has received funding from USAID for the purchase of the initial forensic equipment, as well as for the training and formation of operational teams. It has also collaborated with various competition authorities to exchange experiences and best practices.

38. Furthermore, capacity-building exercises have been held in various jurisdictions, including the APEC Forum, forums organised by the World Bank with the authorities of Malaysia, Morocco, and the Philippines, forums of the Latin American Strategic Partnership for Competition with the authorities of Argentina, Brazil, Chile and Peru, as well as bilateral co-operation with the authorities of Chile, El Salvador and Ecuador. This co-operation has been made possible by the existence of international communication networks, which promote close relationships between competition authorities. Where formal co-operation instruments such as Memoranda of Understanding (MoUs) exist, it is possible to exchange information in accordance with the provisions of this agreement, even allowing knowledge of technical procedures to be shared.

39. In conclusion, digital evidence gathering requires a dedicated data-processing and analysis team, as well as costly storage infrastructure, security and technical capabilities that require constant updating. However, these tools and capacities make it possible to gather information to initiate investigations by virtue of the office held, to collect information during inspections and to identify data that may be useful for investigations and potentially serve as evidence in cases where an opinion of probable responsibility is issued. Considering these benefits, the Commission considers it essential to invest in this capacity to make a substantial contribution to the effective implementation of the LFCE.