Organisation for Economic Co-operation and Development

DAF/COMP/LACF(2020)9

Unclassified

English - Or. English

16 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 Portugal -

28-29 September 2020, virtual Zoom meeting

The attached document from Portugal 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.

JT03465371

Session 1: Digital Evidence Gathering in Cartel Investigations

- Contribution from Portugal -

1. Introduction

1. Combatting cartels has consistently been an enforcement priority for the Portuguese Competition Authority (Autoridade da Concorrência – "AdC" or "Authority"), with the AdC's Competition Policy Priorities highlighting the importance of reinforcing its enforcement activity in the detection, investigation and sanctioning of anti-competitive practices, namely cartels.

2. The increasing digitalization of evidence has, among other advantages, improved the chances of uncovering evidence, particularly during unannounced inspections, thus contributing to the successful conclusion of investigations. However, it has also created novel legal and technical challenges.

3. The policy and approach of the AdC regarding unannounced inspections has therefore evolved over time, reflecting the increasing weight of digital evidence in cartel investigations and addressing the challenges brought by new technologies. Notably, the AdC has modernized its toolbox, improving the collection and analysis of digital evidence by implementing new forensic IT solutions and expanding its related capacity building.

4. The more recent context of COVID-19 also presents challenges to the gathering of digital evidence through inspections. In light of this, procedures may need to be temporarily adapted to exceptional circumstances.

5. In this contribution, we share the AdC's practical experience concerning digital evidence gathering in cartel investigations, providing a background about the applicable legal framework, the AdC's investigative powers and the procedure regarding collection and processing of digital data (Section 2). We share an overview of the related challenges and lessons learned in the digital age, including legal and IT issues (Section 3), and conclude with final remarks.

2. Background

2.1. Legal framework and AdC's investigative powers

6. Under the Portuguese Competition Act[1], the AdC has the power to interview, as well as to request documents and other information from undertakings as well as any natural or legal persons[2].

[1] Law 19/2012 of 8 May.

[2] Articles 15 and 18(1)(a) and (b) of the Portuguese Competition Act.

7. Furthermore, the AdC has the power to carry out unannounced inspections in the premises, property and means of transport of undertakings if such inspections are necessary for obtaining evidence. This includes the power to search, examine, collect and seize data, regardless of the respective storage medium.[3]

8. The AdC also has the power to seal the undertakings' premises where documents and the respective storage medium, "*including computers and other data storage electronic equipment*", are or may be located.[4]

9. In addition, under certain circumstances, the AdC has the power to carry out unannounced inspections at the private homes and other locations, including vehicles, of shareholders, managers and other staff of undertakings.[5]

10. Unannounced inspections require a previous judicial warrant, which is issued by the public prosecutor or by a court. [6] The warrant provides the legal basis for the inspections, defining the respective scope (undertakings and subject matter) and indicating the time limit for carrying out the inspection (maximum of 30 days). If the seizure of evidence found is outside the scope of the warrant, the AdC needs an additional authorization (*ex ante*) or validation (*ex post*) from the judiciary.[7]

11. Information protected by legal and professional privilege ("LPP")[8] cannot be seized during inspections.[9]

12. Under Portuguese law, seizure of mail correspondence which has not been opened is not allowed for the purpose of investigating competition law infringements.[10] The jurisprudence has applied the same rule to electronic correspondence, so e-mails may only be seized if they have been opened.[11]

13. There is no explicit legal deadline for completing the analysis of the evidence collected during inspections. This said, the Portuguese Competition Act provides that, as a general rule, the investigation should be concluded (namely by issuing a statement of objections or filing the case) within a period of 18 months after the decision to open proceedings.[12]

[3] Article 18(1)(c) of the Portuguese Competition Act.

[4] Article 18(1)(d) of the Portuguese Competition Act.

[5] Article 19 of the Portuguese Competition Act.

[6] Article 174(4) of the Penal Procedure Code.

[7] Articles 18(2), 20(1) and 21 of the Portuguese Competition Act.

[8] Under Portuguese law, legal professional privilege covers communications involving either external or in-house counsel under certain circumstances.

[9] Article 180(2) of the Procedural Penal Code and Article 71(1) of the Statute of the Bar Association. See also AdC Procedural Guidelines for Antitrust Proceedings, para. 193, available at http://www.concorrencia.pt/vPT/Noticias_Eventos/Noticias/Documents/LO_Instrucao_Processos_2013.pdf.

[10] Article 179 of the Procedural Penal Code.

[11] AdC Procedural Guidelines for Antitrust Proceedings, para. 52.

[12] Article 24(1) of the Portuguese Competition Act.

2.2. Procedure regarding digital data collection, processing and preservation

14. Some of the main issues concerning digital evidence gathering in cartel investigations take place in connection with unannounced inspections (i.e. dawn raids). In particular, the preservation and protection of the authenticity of evidence during and in the aftermath of an unannounced inspection is crucial for ensuring due process and the successful conclusion of an investigation. With this in mind, the AdC has developed forensic IT skills for the purpose of identifying, collecting, preserving and reviewing digital data in the context of unannounced inspections. The AdC's approach during and after an inspection is subject to constant improvement based on the AdC's experience.

15. One of the first steps during an unannounced inspection is to request the assistance and cooperation of the company's IT manager, as well as to identify the relevant staff of the inspected undertaking, and gather their respective computers or laptops.

16. During unannounced inspections, the AdC will typically seize only a forensic copy of the data which it considers relevant based on a *prima facie* review of the data available at the inspected premises. This review is carried out on the basis of (single or combined) keywords. Furthermore, the use of keywords will help exclude private or LPP-protected information from review and seizure.

17. Under the Portuguese Competition Act, the AdC is required to prepare an official report after the inspection,[13] which shall be notified to the inspected undertaking. It contains a detailed list of the evidence gathered during the inspection, including digital evidence. The latter is identified in the report by making reference to hash files, which constitute proof that the undertaking's files seized by the Authority have not been modified.[14] The AdC procedure also ensures the preservation of data by processing working copies of the digital data to avoid any harm to the original data, with the objective of maintaining a sound chain of custody.

18. When the AdC collects digital files during an inspection which consist in information that is not relevant for the proceedings, it returns those files to the inspected undertaking in the same format in which they were collected.

19. Finally, unless the case is under secrecy of proceedings, any third party showing legitimate interest in the case can request access to the case file.[15]

3. Evidence gathering: challenges and lessons learned in the digital age

20. The AdC's procedure applicable to the gathering of evidence has been adapted in response to the significant exposure to new situations and challenges during dawn raids. Many of these changes also owe to challenges brought by the increasing importance of digital evidence.

21. Therefore, building on its most recent experience with dawn raids, and in the context of strengthening its enforcement strategy, the AdC set up a new model for conducting dawn raids, implementing a number of changes, including:

[13] Article 18(8) of the Portuguese Competition Act.

[14] These files provide a hash value (digital fingerprint) based on algorithms which helps keeping a chain of evidence (proving evidence is extracted from seized data) and chain of custody (proving data provenance).

[15] Article 33(3) of the Portuguese Competition Act.

- Using advanced forensic IT software;
- Providing staff with IT training on a regular basis;
- Deploying more staff per inspection team combining various backgrounds (lawyers, economists and IT experts);
- Increasing dawn raid duration (from 1 or few days to 1-2 weeks);
- Promoting real-time communication between inspection team leaders in different targeted undertakings;
- Providing strong back office coordination and support to inspection teams.

22. The recent context of COVID-19 may present challenges to the gathering of digital evidence through inspections, and thus procedures may need to be temporarily adapted to exceptional circumstances.

23. Besides these changes concerning the approach relating to dawn raids, in the context of digitalization the AdC has also created an online channel which allows for whistleblowers to communicate to the Authority, in an anonymous way, information concerning potential competition infringements.

24. The following subsections focus on the various challenges faced by the AdC before, during and after the inspections, in particular with respect to the digital evidence.

3.1. AdC's forensic IT solutions and related capacity building

25. In general, carrying out unannounced inspections in the era of digitization meant that the Authority had not only to allocate more human resources but also more infrastructure (including rooms dedicated to analysis of evidence) to related tasks. Equally, the AdC did not formally create a separate forensic IT team or unit, but invested significant resources in training staff and providing them with the required tools to tackle the challenges brought by digital evidence.[16]

26. Therefore, the dawn raids carried out in recent years were built on the Authority's investment in (i) capacity building and (ii) advanced IT solutions (both hardware and software), which allowed for speedier processing and reviewing of digital evidence.[17]

27. State-of-the-art hardware and software are costly, so one of the challenges has been to assess on a permanent basis the specific IT needs of the Authority. On the one hand, the Authority seeks to avoid finding itself in a position in which its enforcement initiatives are impaired by a lack of appropriate or sufficient IT solutions. On the other hand, financial resources need to be managed rationally, and unnecessary IT costs should be avoided. In practical terms, this translates for example in understanding how many software licenses of the forensic IT software the Authority needs to have in place on a yearly basis so that, if need be, it is able to deploy the necessary IT resources within a short notice period.

[16] The process of investing in forensic tools and capacity building benefitted from the international cooperation between the AdC and other competition authorities in the context of the European Competition Network and the International Competition Network, for example with participation of AdC staff, including the IT staff, in unannounced inspections carried out jointly with other competition authorities.

[17] Besides higher processing speed, advanced forensic IT software provides for user-friendly filters which allow to remove duplicates, filter e-mails, highlight keywords in documents, tag documents, aggregate e-mail threads, extract lists showing patterns per target, year or tag, etc.

28. In addition to acquiring IT software licenses, it is also necessary to provide the necessary training to staff. In the AdC's experience, there are at least two target groups with different needs: (i) specialized forensic IT staff, whose training includes learning to manage and adapt the software to the procedure applicable in the dawn raids and any specific circumstances;[18] and (ii) Authority staff in charge of reviewing the data at the inspected premises (and later, at the premises of the Authority), who should learn skills necessary for the purpose of the document review (e.g. select datasets, create keyword strings, save searches, etc). Since the latter involves more basic skills, this staff can be trained in-house by the specialized forensic IT staff.

29. Overall, on the basis of the AdC's experience so far, the benefits brought by the investment in advanced forensic IT solutions and related capacity building appear to outweigh costs. This is not only because such solutions save time, allowing for the review of a larger set of evidence in a shorter period of time, but also because in doing so they enable structural changes regarding the way the authorities may organize dawn raids and even, more generally, their investigations.

3.2. Legal issues and other challenges related to digital evidence

3.2.1. Unopened e-mails

30. As already mentioned, in Portugal unopened e-mails cannot be seized under proceedings relating to competition law infringements. This framework stems from the regime applicable to physical mail correspondence and is ultimately based on a constitutional right.[19]

31. While nowadays the volume of physical mail is negligible, e-mail has become the preferred professional communication tool in the past two decades. Therefore, this rule may have a significant impact on the Authority's ability to gather relevant evidence.

32. Furthermore, it is unclear whether so-called "unread e-mails" deserve the same protection as unopened physical mail, given that it is difficult to ascertain whether an "unread e-mail" has been opened or not.[20] In this respect, the implementation of the so-called "ECN+ Directive", intended to empower national competition authorities in the Member States of the European Union (EU) to be more effective enforcers, may help change this situation as it advocates for providing authorities with the necessary powers to gather all relevant evidence during inspections when enforcing Articles 101 and 102 of the Treaty on the Functioning of the European Union.[21]

[18] Typically, this staff accumulates forensic IT tasks with a more general IT role, being in charge of communication with IT counterparts at the inspected undertaking and the identification and collection of data from relevant staff.

[19] Article 34(4) of the Constitution of the Portuguese Republic.

[20] Programs used for sending, receiving and reading e-mails allow users (i) to read at least part of the content without automatically marking the e-mail as "read" and (ii) to mark messages as "unread" after reading them.

[21] Directive 2019/1 (EU) 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.

3.2.2. Due process challenges: confidentiality issues

33. The gathering of large amounts of digital evidence also raises issues relating to the protection of confidential information, as it is necessary to avoid a burdensome access to file procedure, while striking a balance between ensuring the rights of defense and protecting confidential information.

34. The Portuguese Competition Act establishes the framework for the protection of business secrets in the context of unannounced inspections and other fact-finding measures[22]. Confidentiality is particularly relevant in the context of access to file. It is also relevant upon the publication of decisions, as the AdC has the duty to publish on its internet website the non-confidential version of its final infringement decisions[23]. Parties may make confidentiality claims, providing, in such case, a copy of the documents with the confidential information expunged. The AdC may (or may not) agree with the classification of the information as a business secret and shall hear the involved parties, before adopting its decision. In any event, the parties' external lawyers and economic advisers may have access to confidential documents for the exercise of the rights of defense and judicial appeal.[24]

35. Within this framework, the AdC has sought to ensure a fair balance between rights of defense and the protection of confidential information while keeping the procedure as less burdensome as possible, in particular taking into account the increasing amount of available digital evidence in antitrust proceedings. In this context, appeals brought by parties have tested the AdC procedure, hinging, for example, on whether the AdC was allowed to ask parties to produce summaries of the information considered confidential[25], and whether the AdC was right to forbid undertakings from obtaining copies of documents which only their external lawyers and economic consultants could review[26].

4. Concluding remarks

36. The Portuguese Competition Act provides the AdC with a comprehensive set of powers to gather digital evidence in cartel investigations, in particular through unannounced inspections.

37. Nevertheless, the gathering and collection of evidence in the digital era presents the AdC with both opportunities and challenges.

38. Therefore, the AdC has over time implemented a significant overhaul of its dawn raid procedures, tools and resources with a view to strengthen its enforcement. In light of the importance of digital evidence, it proved crucial to invest in advanced forensic IT solutions and capacity building, as well as to adapt the procedures to the challenges brought by new technologies and digital evidence.

[22] Articles 15 and 30 of the Portuguese Competition Act. See also AdC Procedural Guidelines for Antitrust Proceedings, paras. 176-192.

[23] Article 90(1) of the Portuguese Competition Act.

[24] Article 33(4) of the Portuguese Competition Act.

[25] Competition, Regulation and Supervision Court, first instance, 25.10.2016, Case no. 195/16.1YUSTR.

[26] Lisbon Appeal Court, second instance, 05.04.2016, Case no. 225/15.4 YUSTR.L1.

39. Furthermore, the implementation of the "ECN+ Directive", intended to empower national competition authorities in the EU Member States to be more effective enforcers, will reinforce the digital toolbox of the Authority as the Directive advocates for providing authorities with the necessary powers to gather all relevant evidence, including digital evidence, when enforcing Articles 101 and 102 of the Treaty on the Functioning of the European Union.[27]

[27] Directive 2019/1 (EU) 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.