Organisation for Economic Co-operation and Development

DAF/COMP/LACF(2020)7

Unclassified

English - Or. English

10 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 Costa Rica -

28-29 September 2020, virtual Zoom meeting

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

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

JT03465106

Session 1: Digital Evidence Gathering in Cartel Investigations

- Contribution from Costa Rica[*] -

1. Introduction

1. Currently, with the evolution of information technologies, society is quite easily participating in commercial transactions (E-commerce), communicating through smartphone applications, and managing personal and even business matters through social media. This calls for a tool that can easily be updated and quickly be adapted to any change.

2. In face of this new information reality, traditional proof of evidence are now being displaced by other sources, electronic in nature, moving us from physical paper to electronic documents stored in digital devices or in the cloud, e-mails, instant messaging through smartphone applications, in order to exchange files, voice messages, photographs, and others. Additionally, calls to mobile phones or landlines are also being displaced by new applications, such as text messages, that only require a good Internet connection.

3. In this sense, conversations via Whatsapp, Facebook or Instagram, or through email or other such means, may be decisive for competition authorities to prove the existence of absolute monopolistic practices (hard core cartels) between and among economic agents in order to, most often, undertake acts of collusion.

2. Powers to Gather Digital Evidence

4. The national competition authorities are responsible for addressing these practices in different areas. Costa Rica has two different authorities in charge. The first, the Commission for the Promotion of Competition (Comisión para Promover la Competencia - COPROCOM), is assigned to the defence and promotion of competition and free concurrence in other matters. And the second, the Superintendence of Telecommunications (Superintendencia de Telecomunicaciones - SUTEL), is the sectorial authority in charge of the defence and promotion of competition and free competition specifically in the telecommunications sector.

5. Ever since their creation, COPROCOM and SUTEL were given the legal mandate to sanction, as provided in Article 11 of the Law for the Promotion of Competition and Effective Consumer Defence, Law 7472, and Article 53 of the General Telecommunications Law, Law 8642; however, prior to 2019, they lacked the necessary tools to adequately detect cartels.

6. With the enactment of the Law for the Strengthening of Competition Authorities of Costa Rica, Law 9736, both authorities are now authorized to perform inspections, with prior authorization of the Administrative and Civil Treasury Court, to inspect industrial or commercial establishments, or other personal and real property, as necessary, to gather, or

[*] This document was prepared by COPROCOM (National Commission for the Promotion of Competition) and SUTEL(Superintendency of Telecommunications) .

prevent the loss, or destruction, of evidence for an investigation related to absolute or relative monopolistic practices.

7. Once a request is lodged with, and reviewed by, the Administrative and Civil Treasury Court, as applicable, it will authorize such inspection, and will determine the scope, objectives and specific site(s) of the action.

8. Inspections follow a special pre-established procedure in order to determine the existence of an absolute monopolistic practice, either during the preliminary investigation or pre-trial phase, or when there are signs of evidence relevant to the investigation, which could be in the hands of one or more economic agents, object or not of the investigation, or when there is danger that, absent an inspection, the evidence might not get incorporated into the investigation, and end up lost or destroyed.

9. Having described the scope of official inspections, it is worth explaining the scope of the inspection process itself. Once the Court authorizes an inspection, the authorities may go to the facilities or offices of the economic agents and demand access to accounting books, documents, contracts, correspondence, files, visitor records, worker schedules, e-mails, external storage hard drives, and any other information that may be held in physical documents or electronic files, regardless of format, type of file or storage device used, provided they are related to the object of the investigation and are mentioned in the legal inspection authorization.

10. It is worth highlighting that Law 9736 authorises both COPROCOM and SUTEL to gather evidence in digital format during cartel detection and investigation proceedings.

11. Also noteworthy is the fact that officers and staff at the inspection site must accept the process and collaborate reasonably, and must refrain from acting in any manner that may unjustifiably interfere with, or delay, the process. They must also provide any information and documentation requested and must give access to offices, computers, books, storage devices, filing cabinets, or any other asset and/or physical or digital element that may contain such information.

12. Inspectors are authorized to interview and ask assistance from employees, representatives, directors or shareholders present at the time of the visit to ascertain the existence and location of any information and/or documents relevant to the investigation. These individuals must promptly provide any information that may help locate relevant materials and documents.

13. The economic agent, or its legal representative, may be present at the time of an inspection and, at that time, may make any comments it deems appropriate regarding the actions of the authority, and these are reflected in the corresponding report. A legal adviser may be present during this process. The absence of a representative or legal adviser of the economic agent during the inspection does not impede such inspection.

14. During an inspection, reasonable suspicion may arise about important evidence being held elsewhere, at other industrial or commercial establishments or in other personal or real property of the economic agent, and which could help prove a monopolistic practice. In such event, the Higher Body of the corresponding competition authority may ask the relevant judicial authority to broaden the authorization in order to inspect those other establishments or properties.

15. It is worth noting that all officers from the corresponding competition authority participating in the process must hold confidential any information they may receive before or during the process. Therefore, the execution of an inspection, and its details, and any documents or decisions related thereto shall be confidential and kept private by the corresponding Body depending on the inspection phase.

16. Now, specifically in reference to evidence gathered in the investigation and pre-trial process carried out by the competition authority, Article 40 of Law 9736 provides that, during the investigation phase, the dossier or file must contain all evidence provided by the complainant and, if applicable, evidence gathered during the preliminary investigation.

17. Article 47 of that same Law provides that any means of evidence admissible under public law shall be accepted in the pre-trial phase, even though not admissible under common law. Any evidence offered by the parties in a statement of defence, or later, and/or held by the examining body, must be added to the dossier/file, duly numbered, and in the chronological order received.

18. In summary, evidence allowed for under common law is admitted in any of those phases, and will be examined under the rules of sound criticism. Regarding electronic evidence, the legal system itself has equated physical evidence and electronic evidence, provided there is also functional equivalence, as indicated above. Therefore, this evidence is also valid in these proceedings.

19. As will be further explained in the next section, electronic evidence has been admitted by the Costa Rican judicial and administrative authorities as a means of evidence in proceedings as provided in regulations that assign functional equivalence to both electronic and physical documents, unless the evidence was not gathered through valid means.

20. The admission of digital evidence could be decisive to resolve processes confirming absolute monopolistic practices between or among economic agents for collusive purposes since, as indicated above, electronic documents are equivalent to physical documents, provided they meet functional equivalence. Clearly, acceptable means of lawful evidence have evolved, not only physical documents, but also telephone calls and modern platforms.

3. Digital Evidence in the Field of Law in Costa Rica

21. Having analysed competition and the breadth of powers of the Costa Rican competition authorities, particularly for inspections, it is appropriate to refer to electronic evidence as such, and how it has been accepted in national investigations, from administrative to criminal.

22. The Costa Rican legal system does not provide an express definition of the comprehensiveness of evidence gathered from new information and communication technologies. However, it is clear that electronic evidence will be subject to the same evidence-related elements, theory and principles as any other type of evidence.

23. Several definitions have been produced for "digital evidence." The first was developed by the Federal Bureau of Investigations (FBI) in 2000 through the "*Standards and Principles - Scientific Working Group on Digital Evidence,*" indicating *"Information of probative value stored or transmitted in digital form."*[1]

24. The term has also been conceptualised as *"any information obtained from an electronic device or digital medium which serves to convince the truth of a fact."*[2]

[1] Federal Bureau of Investigation, Digital Evidence: Standards and Principles (Federal Bureau of Investigation, 2000)

[2] https://adefinitivas.com/wp-content/uploads/2019/04/la-prueba-electrc3b3nica-un-medio-de-prueba-desconocido-1.pdf

25. In 2005, Costa Rica enacted the Law of Certificates, Digital Signatures and Electronic Documents, Law 8454, which encompasses all types of transactions and legal acts, public and private, unless otherwise provided by law, or unless the nature, or specific requirements, of the concrete act or business are incompatible.

26. The novelty of this law is that it recognizes the functional equivalence of electronic documents, defined as follows:

> *"**Article 3.-Recognition of functional equivalence** - Any manifestation, representative or declarative in nature, expressed or transmitted through an electronic or digital medium shall be understood as legally equivalent to documents issued by, residing in, or transmitted via, physical means.*
>
> *Any regulation in the legal system that refers to a document or communication shall be understood to include electronic and physical documents or communications. Nevertheless, the use of an electronic form for a given document will, in no case, exempt from compliance with lawful requirements and formalities applicable to every legal business or act in particular."*

27. Likewise, Article 4 of that same Law classifies electronic documents as public or private and **of probative value under the same conditions as physical documents.** The Regulations to such Law, namely Article 2, define the concept of electronic document as *"any manifestation, representative or declarative in nature, expressed or transmitted through an electronic or digital medium."*

28. In line with Article 3 of Law 8454, the Organic Law of the Judicial Branch, Law 8, reaffirms the principle of functional equivalence in Article 6 bis, which reads:

> *"**Article 6 bis**.- Files containing documents, messages, images, bank data and all applications stored or transmitted through electronic, digital, magnetic, optical or data transmission means or produced through new technologies destined for legal proceedings, containing judicial acts or resolutions shall have the same validity and efficacy as an original physical document. This applies provided that the established steps have been taken to ensure their authenticity, integrity and protection. Any alteration that may affect the integrity or authenticity thereof shall result in the loss of its legal value as provided in the previous paragraph.*

29. In line with the above, since 2005 the Costa Rican legal system provides that any manifestation, representative or declarative in nature, made through an electronic medium has the same validity as a physical document.

30. As criminal matters, in Costa Rica, electronic sources of evidence are considered documents. Article 1 of the Law on the Registration, Seizure and Examination of Private Documents and Intercepting Communications (Law 7425) expressly indicates:

> *"**Article 1.-Competency.** For purposes of the Law herein, private documents are: correspondence by means of written correspondence, fax, telex, data transmission, or any other means; videos, cassettes, tapes, disks, diskettes, writings, books, memorials, records, plans, drawings, paintings, radiographs, photographs and any other form of recording information of private character, used with declarative or representative intent, to illustrate or prove something."*

31. As indicated, electronic evidence in a criminal proceeding is equivalent to documentary evidence because it fulfils the requirement of being declarative and/or representative, precisely the key aspect of a document. Moreover, it is important to indicate that any electronic evidence contained in a private digital device is considered a private document, and is therefore subject to seizure under a criminal process, regardless of the offence.

32. One example of such type of evidence in a criminal proceeding appears in Resolution 558 of the Criminal Court of Cassation of San Ramón, when determining that the *SIM card* in a mobile telephone is considered a document. The Resolution reads:

> *"Now, regarding the concept of private documents, this is not the traditional concept of document but instead a broader concept, that is, a medium in which any type of private information can be stored or recorded. Besides listing the types of documents stricto sensu, such as books, writings, memorials, etc. mention is also made of any form of recording information of a private nature, used with declarative or representative intent, to illustrate or prove something. For the matter herein, there is no doubt that* ***the SIM cards removed from the cellular phones confiscated from the defendants constitute a form or means to record information of a private nature since, through such means –the SIM cards- not only is it possible to store data related to the telephone service (telephone information such as its number), but also other data or information, of a private nature, that exclusively belongs to the user or owner of such telephone.*** *When information contained in such a medium is demanded, this is not in itself an event of intervention of communication, since the objective is not to determine what a person discusses or has discussed with another person. The only objective is to determine the contents of data or information stored in this electronic form. Thus, in this case, the contents of Article 2 through 4 of the abovementioned regulation had to be observed since they clearly indicate the formalities and procedures to follow in this type of process. Here it is important to remember that the Political Constitution recognises and guarantees an intangible sphere of privacy with respect to private, personal or sensitive data that may be held in different files or systems (electronic or otherwise). This means that such records cannot be violated and* ***the only manner in which this can occur is with a corresponding jurisdictional order issued by the corresponding competent authority****. Said order must fulfil all the requirements and formalities provided by law and in the Political Constitution. (...)" (Criminal Court of Cassation. Vote number 551 at 10:00 hours of 21 November 2008).*

33. Regarding instant messaging apps, like *WhatsApp*, these have also been used as evidence in different proceedings, so it could be held that the exchange of such conversations, images and even documents is limited to the individuals in that conversation (issuer and recipient), and there could eventually be a violation of Constitutional rights, namely the right to privacy, when such conversations are accessed by third parties totally foreign to the conversation without using an adequate digital evidence collection mechanism, as provided in Law 9736.

34. In particular, the Constitutional Chamber resolved, in 2018, an appeal lodged against the Caja Costarricense del Seguro Social claiming the violation of Article 24 of the Political Constitution when a conversation held via WhatsApp was brought as evidence without judicial authorization, turning its collection into an unlawful act.

35. Under Vote 7460 of 09:45 minutes of 11 May 2018, the Constitutional Chamber resolved the *amparo* petition as follows:

*"**III.-On the Merits**. In the case under review, the appellant states that he is the subject of a disciplinary procedure... He claims that the proceeding utilised as evidence a WhatsApp conversation which was collected without the authorization of a judge. When examining a similar case, this Chamber ordered in Ruling number 2015-13737 at 12:01 of 28 August 2015, the following:*

***" I.- Object of the petition**. The appellants claim that, based on private communications in a WhatsApp group they are members of, the Judicial Inspection Court has initiated an administrative disciplinary procedure against them, which they consider adversely affects their rights, and therefore they request that their petition be declared admissible, with its consequences. (...)*

***III .- On the Merits.** As is apparent in this case, the issue under discussion herein deals with one of the new technologies now available to individuals and, through its use, problems are now arising that bring about consequences, the legal nature of which must be resolved despite the scarce legislation regarding such novel matters. In this concrete case, the Chamber is being presented with an effect caused through the use of the WhatsApp tool, and the Chamber must analyse whether the argument posed by the appellants is indeed an adverse impact on their basic right to personal privacy and privacy of communications. It is first necessary to indicate that WhatsApp is an instant messaging application for smart phones, to send and receive messages via the Internet, supplementing e-mail services, instant messaging, short message systems (SMS) or multimedia messaging systems. Besides using text messages, users of the Contact list may create groups and send each other images, videos and audio files. This tool is broadly accepted worldwide which (...) continues to grow, and is currently considered the instant messaging service par excellence, reaching more and more corners of the planet every day, with more that 600 million active users. Since this is a messaging service available on cellular telephones which are, no doubt, for personal and private use, logic would indicate that the personal and private modifier also applies to the device and, therefore, the contents therein are private and belong to the telephone owner, who can determine who else may have access thereto. To this effect, it is worth recalling that this Chamber has categorically indicated that Article 24 of the Political Constitution and Article 11 of the American Convention on Human Rights enshrine the right to privacy which, among others, aims to assure each individual a personal space, a private sphere inaccessible to the public, except as expressly allowed by the interested party; this assurance protects the freedom of communication and prohibits third parties –public or private- from intercepting or taking over third-party communications in an unlawful manner (down these lines, and among others, see Ruling Number 2014-018952 of 9 hours and 05 minutes of 21 November 2014). This sphere protects the private lives of citizens. Privacy consists of events, behaviours, information and situations about an individual not normally known to others but which, if revealed, would morally upset the individual, affecting his/her discretion and modesty, unless revealed upon consent of that individual. Events occurring inside the home of a citizen are, no doubt, considered private, as well as inside offices, homes of friends and other private areas. In this manner, the Constitutional rights of inviolability of the home, of private documents and of communications exist precisely to protect said privacy, a basic right of each individual. Home and communications can only open up for a fair and concrete cause. The same applies to privacy in general since, as indicated in the American Convention on Human Rights, Article 11, paragraph 2: "... No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his written correspondence, or of unlawful attacks on his honour or reputation..." (See, among others, Ruling number 1026-94 of 10 hours 54 minutes of*

18 February 1994). Therefore, the protection granted under Article 24 is such that public authorities cannot enter that private sphere without a legal order.

*IV.- (...) It is also established that the complainants, through the technology provided by the abovementioned WhatsApp mobile application, formed a private contact group for the exclusive use of its members, where they displayed images and conversations, sexual in nature, which apparently affect their female co-workers, the complainants. The disciplinary file shows that one member of said WhatsApp group collaborated with the disciplinary investigation and provided the images and conversations that affected the complainants; this information has allowed opening a disciplinary investigation against the defendants for alleged sexual harassment. Additionally, this person also authorized the extraction of such evidence from his mobile phone. For the Chamber, in this concrete case**, **no court order is required to inspect the contents of telephone conversations held by the group since one member of the WhatsApp group gave his consent for the Judicial Inspection Court to access the information, which served to open an investigation against the defendants. This person collaborated with the disciplinary investigation, provided images and conversations to be used as evidence, and authorised their extraction from his mobile telephone, although the information contained was confidential to other group members. Thus, this Court deems that access to such information by the Judicial Inspection was valid despite being held in the private, intimate and confidential scope of the group members, one of which disclosed the information and voluntarily made it available, and even collaborated with the investigation, a fact that cannot be considered a violation of the right to privacy and the inviolability of communications, guarded in Article 24 of the Constitution.** *Consequently, since the facts presented are not in violation of the basic rights of the appellants to privacy and inviolability of private communications, it is appropriate to dismiss the appeal, as in fact is ordered."*

IV.-Now, an analysis of the documents shows that the WhatsApp conversation contested in the libel file was made available by one individual that was part of such conversation and also appears as complainant in the administrative proceeding 16-17. ***Therefore, and in line with the contents of the pronouncement indicated in the previous recital, it is not necessary to have a court order to access such message since it was voluntarily presented by an individual who participated directly in the conversation, and who gave his consent for its use as evidence in the abovementioned administrative proceeding****. With this, the Chamber does not consider there is a violation of Constitutional Article 24, and the appeal must be dismissed.*

(...)" (Highlighted text is intentional)

36. For this case, it is important to rescue two points: first, the freedom to offer an electronic conversation as evidence and, second, the consent granted to incorporate such evidence into the administrative record.

37. These two points were fundamental to determine the appeal. The Constitutional Chamber ruled there was no violation of Article 24 of our Political Constitution, related to the right to privacy and secrecy of communications, since consent had been granted to access such information. In the same lines, the claim about a violation of such right is unfounded because the recipient himself of the conversation uses that information to support a specific complaint.

4. On adjustments required to gather digital evidence in the field of competition law in Costa Rica

38. Finally, it is important to discuss the actions to be taken by the Competition Authorities concerning the implementation of tools that may assist with the collection and analysis of electronic evidence.

39. As part of the actions aimed at institutional strengthening, the Competition Authorities have developed a roadmap for the implementation of Law 9736. The plan lays out a series of general and specific actions for the forthcoming years.

40. The roadmap, designed by both authorities, contains three major pillars: the first is a stronger regulatory framework, the second is more robust institutional capacity, and, third, more effective law enforcement.

41. The first pillar requires developing the necessary secondary or supporting legal instruments to ensure due process in any internal proceeding related to inspections. The second pillar, namely institutional capacity building, requires developing necessary actions related to the digital infrastructure required by COPROCOM and SUTEL for purposes of most adequate law enforcement.

42. As discussed throughout this document, Costa Rican legislation provides that, to ascertain the validity of a piece of evidence in an administrative or judicial proceeding, this evidence must have been gathered through the appropriate lawful mechanisms.

43. Thus, regarding digital evidence, unless brought into the case directly by a party involved, a court authorisation is required to collect it, through an unannounced inspection.

44. During such inspection, all elements of due process must be observed, such as, among others, use the appropriate removal and safeguard mechanisms and tools, and guarantee the chain of custody of such evidence.

45. To comply with the above, adequate mechanisms are necessary, not only regulatory (like internal procedures and guidelines to ensure that unannounced inspections to gather any such information and documents observe all relevant procedural principles), but also technological (with adequate instruments to capture digital information).

46. Throughout 2020 and 2021, COPROCOM and SUTEL plan to produce the necessary guides and manuals to assist with surprise inspections, including how to capture digital evidence, particularly to prosecute cartels.

47. Another general action deals with the provision of technological capabilities. The abovementioned roadmap includes the purchase of hardware and software for digital forensic analyses, a task under the responsibility of both authorities, and the design of the system itself. This should be executed in 2023 through an administrative contract process. The systems purchased would then be assigned to both authorities.

48. With the necessary legislative and technological capabilities, it is expected that both SUTEL and COPROCOM with be able to better collect digital evidence, in full compliance with the legal principles in force in the country.

Bibliography

Ley de Fortalecimiento de las Autoridades de Competencia de Costa Rica (Ley 9736)

Ley de Certificados, Firmas Digitales y Documentos Electrónicos y su reglamento (Ley 8454)

Ley Orgánica del Poder Judicial (Ley 8)

Ley de Promoción de la Competencia y Defensa efectiva del consumidor (Ley 7472)

Ley General de Telecomunicaciones y su reglamento (Ley 8642)

Ley sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones (Ley 7425)

Tribunal de Casación Penal. Voto número 551 de las 10:00 horas del 21 de noviembre del 2008

Sala Constitucional. Voto número 7460 de las 09:45 minutos del 11 de mayo del 2018

Federal Bureau of Investigation, Digital Evidence: Standards and Principles (Federal Bureau of Investigation, 2000)

Prado, J. (2019). *La prueba electrónica, un medio de prueba desconocido*. In A DEFINITIVAS. https://adefinitivas.com/wp-content/uploads/2019/04/la-prueba-electrc3b3nica-un-medio-de-prueba-desconocido-1.pdf