Organisation for Economic Co-operation and Development

DAF/COMP/WD(2020)42

Unclassified

English - Or. English

14 May 2020

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Consumer data rights and competition – Note by Colombia

12 June 2020

This document reproduces a written contribution from Colombia submitted for Item 3 of the 133rd OECD Competition Committee meeting on 10-16 June 2020.

More documents related to this discussion can be found at
http://www.oecd.org/daf/competition/consumer-data-rights-and-competition.htm

Please contact Ms Anna BARKER if you have questions about this document.
[Email: Anna.BARKER@oecd.org]

JT03461726

Colombia

1. Data can provide economic and competitive benefits to market agents. It can play a pivotal role in many actors' strategic decision-making processes and can certainly be considered as a competitive advantage over rivals. Many companies collect large amounts of personal data, others process it and some more buy and sell it.

2. Data-driven businesses have recently raised the attention of competition authorities. Their interactions and dynamics are likely to implicate competition concerns. Even though every agent or third party who processes and controls personal data in any amount, as well as the way it does so is relevant to Data Protection enforcers to begin with, it may not be significant in the same degree to Competition or Consumer protection enforcers. The debate regarding the extent to which data-related dynamics can be analysed into the assessment of potential harms to competition and consumers is timely and thought-provoking. We believe that the premise for the assessment of whether a certain market is functioning properly is still the same: to consider every variable that is at play and every potential violation to regimes that are different in nature but that at the same time have a complementary role in achieving the wellbeing of consumers and the market itself.

3. According to the OECD's Background Note prepared by the Secretariat for the present Roundtable, the term "consumer data" is "intended to capture data concerning consumers, where such data have been collected, traded or used as part of a commercial relationship". This concept appears to be narrower than the one of "personal data", which under Colombian regulation covers "any information relating to or that may be associated with a determined or determinable natural person" which not necessarily is limited to a commercial relationship. In another sense, it is also broader than personal data, for it may consider information collected, used and disclosed in the context of a commercial relationship but that cannot be traced back to a specific data subject as the personal data definition requires.

4. Colombian data protection regulation does not consider explicitly the term "consumer data". However, the term "personal data" as defined by the law covers the category abovementioned to the extent that data concerning an identified or identifiable natural person. The regulation does not cover anonymous data.

5. This submission discusses the state of play of the protection of data rights of consumers under the Colombian Data Protection, Consumer Protection and Competition Protection Regimes. To that effect we will present the way those rights are interpreted and enforced under our applicable regulations. We will provide a short description of the concepts that are key to the present discussion from our jurisdictions perspective and finally we will address the role of both Consumer Protection and Competition Protection enforcement and advocacy actions towards the protection of those rights.

1. Colombian Data Protection Regime

6. The Colombian Data Protection Regime (Law 1581 of 2012, General Data Protection Regulation, and others) develops the constitutional rights of all persons to know, update and rectify the information that has been collected about them in databases or archives, as well as the rights, freedoms and guarantees referred in articles 15 of the Constitution (protection of personal data, privacy and good name) and 20 (right to access to information).

7. The regime also includes other regulations like the Law 1266 of 2008 –also known as the "Credit Reporting Act"– and the chapter 25 of the Decree 1074 of 2015 which partially regulates Law 1581 of 2012. Under such provisions, private organisations and public entities must respect several key rules, including data protection principles – lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, access restrictions, and security and confidentiality –, cross-border data transfer requirements, data subject rights, and obligations.

8. The type and amount of personal data an organisation or a public entity may process depends on the reason for processing it (legal reason used) and the intended use. However, the accountability principle provides that data controllers are responsible for the personal information under their control, much of which is sensitive (Articles 2.2.2.25.6.1. and 2.2.2.25.6.2 of Decree 1074 of 2015).

2. Key concepts from Colombia's jurisdiction perspective

9. The protection of natural persons in relation to the processing of personal data is a fundamental right (this right is known as "habeas data"). Articles 15 and 20 of the Political Constitution of Colombia establish that data subjects (or individuals) have the rights of information, access to and rectification or removal of personal data concerning them collected, used or disclosed or otherwise processed by private companies and public authorities. The Article 15 provides that the processing of personal data must respect the rights, freedom and guarantees provided by the Constitution.

10. Although the right to the protection of personal data is closely linked to the rights to privacy and good name, respectively, Article 15 recognizes them as fundamental rights with autonomous and different content. In any case, the misuse of personal data could lead to physical, material, or non-material damage, in particular, where data subjects might be deprived of the rights to protection of privacy and good name. If individuals think that their rights to privacy and good name were allegedly violated they may claim legal protection before any judge, at any time or place, through a preferential and summary proceeding (Article 86 of the Political Constitution of Colombia).

11. Personal data means any information that relates or can relate to an identified or identifiable individual (Article 3 (c) of Law 1581). Different factors can identify an individual (data subject). Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (Article 4 of Law 1581).

12. Where the processing is based on the data subject's consent, organisations should be able to demonstrate that the data subject has given prior informed consent to the processing operation (Articles 9, 10 and 12 of Law 1581). Explicit consent will be necessary for the use of sensitive data and children's data, unless an exception applies (Articles 5, 6 and 7 of Law 1581). For consent to be informed, the data subject should be aware at least of the identity of the organisation and the purposes of the processing for which the personal data are intended. Unfair or deceptive acts or practices cannot be used to collect and process personal data (Article 2.2.2.25.2.1 of Decree 1074 of 2015).

13. Personal data can only be transferred from Colombia to another country when an adequate level of protection is guaranteed under Law 1581, unless an exception applies (Article 26 of Law 1581). Where any organisation fails to fulfil its obligations, the Superintendence of Industry and Commerce (SIC) through the Deputy Superintendence for the Protection of Personal Data has the following powers, among others:

1. to issue orders to organisations that intended processing operations are likely to infringe provisions of the regulation.
2. to order organisations to comply with the data subject's requests to exercise his or her rights.
3. to order organisations to bring processing operations into compliance.
4. to impose a temporary or definitive limitation including a ban on processing.
5. to order the rectification or erasure of personal data.
6. to impose an administrative fine.

14. In decision No.74828 of 17 December 2019, the Delegate for the Protection of Personal Data found that RAPPI, a e-commerce food delivery company and marketplace, failed to demonstrate that a data subject had consented to the processing of his or her personal data for marketing and advertising purposes.

- The Delegate ruled that the creation of a user login on a technological platform does not mean, per se, that the data subject has consented the processing of his or her personal data. Besides, the authority said that a privacy notice does not replace the obligation of an organisation to obtain valid consent.
- RAPPI also failed to respond to a request for erasure within 15 working days of receipt (Article 15 of Law 1581) – RAPPI took more than twenty-two months (22 ½) to delete the data subject's information.
- In light of the above, the Delegate concluded that RAPPI did not implement policies and practices to give effect to the data protection principles under Law 1581 of 2012. This is particularly concerning given the vast amount of personal information under RAPPI's control.

15. The Deputy Superintendence for the Protection of Personal Data is not competent to order organisations to compensate for any damage which a person may suffer as a result of processing that infringes Law 1581 of 2012. Therefore, a data subject (or individual) who has suffered material or non-material damage or interference with her/his rights and freedoms has the right to file a lawsuit before a civil judge to obtain the compensation they deserve.

16. Unlike the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), Colombia does not yet have the right to data portability. However, Article 15 of Law 1581 and Article 2.2.2.25.4.2 of Decree 1074 of 2015 establish that organisations shall establish mechanisms to ensure the right of access to personal data. As a good practice, organisations can provide the information requested by the data subject in a structured, commonly used and machine-readable format. This mechanism would offer an easy way for data subjects to manage and reuse personal data themselves.

3. Role of Consumer Protection law enforcement

17. Regarding Consumer Data Rights, from the perspective of the Colombian Consumer Protection Statute – Law 1480 of 2011, there are three main areas that elucidate the relationship between the regimes of personal data protection, consumer protection and competition. All of these areas emerged from new technologies within e-commerce markets, answering to the need to reach efficiency when trading goods and services *via* online.

3.1. The construction, processing and use of big data to deliver personalised advertising and prices.

18. Personalised advertising is one of the main commercial uses for the collection, process and application of personal data, which is a practice that has been named as "Online Behavioral Advertising (OBA)".

> *OBA relies on the tracking of consumer behaviour online. Traditionally, "cookies" (essentially a bit of digital code that records certain user behaviour) have been used to track online behaviour via desktop browsers. Cookies can be first-party or third-party. First-party cookies originate from (or are sent to) the website the consumer is currently viewing, whereas third-party cookies originate from (or are sent to) an unrelated website*[1]

19. By tracking consumers' online behavior, companies can create detailed and individual profiles to use for targeted ads, see how consumers interact with those ads and use this information as a starting point to improve consumers' experience in e-commerce. This is mostly the "pretty face" of this technology, which at first sight would not infringe consumer rights under Colombian Legislation. Nonetheless, the abuse of behavioral insights tools and applications can seriously endanger consumer rights by nudging them into a purchase and by those means possibly violating their right to freely choose the goods and services.[2]

20. The SIC participated last year in an investigation activity within the framework of the International Consumer Protection and Enforcement Network (ICPEN). In 2019, this activity named the "sweep", focused on the analysis of behavioral insights tools that could mislead consumers. For this sweep the SIC investigated and analysed different economic sectors within digital economy, namely, (i) tourism platforms, (ii) hotels, (iii) market places offering goods, (iv) anti-virus software, (v) car rentals, (vi) videogaming websites, (vii) telecommunication services sold online and (viii) postal services. For each sector, five (5) web pages were reviewed whose administrator and owner was domiciled in Colombia.

21. Several examples were found of the use of abusive practices of consumer rights, especially the right to free choice, where the theory of "behavioral economics" was used to manipulate consumer decisions. An example of this is the *pressure selling* technique, where the website sets a descending timer indicating the hours, minutes, seconds and thousands, when the promotion ends. This practice is used to manipulate the unconscious part of the brain and encourage it to buy something that may not meet its needs, at least from the perspective of the *homo economicus*[3] of classical economic theory.

22. Currently, the SIC is closely monitoring these new technologies and has been preliminary analysed whether it violates Consumer Protection Law.

3.2. The fraudulent collection of data by means of non-monetary transactions

23. Non-monetary transactions are defined by the OECD E-commerce recommendation in the following terms:

[1] OECD (2019), "Online advertising: Trends, benefits and risks for consumers", OECD Digital Economy Papers, No. 272, OECD Publishing, Paris, https://doi.org/10.1787/1f42c85d-en.

[2] Article 3 of the Colombian Consumer Protection Statute –Law 1480 of 2011.

[3] 'Vista De Economía Del Comportamiento: Pasado, Presente Y Futuro' (*Revistas.uexternado.edu.co*, 2020) <https://revistas.uexternado.edu.co/index.php/ecoins/article/view/5271/6402> accessed 6 May 2020.

> *Consumers increasingly acquire "free" goods and services in exchange for their personal data and these transactions are now explicitly included in the scope of the Recommendation.*[4]

24. Non-monetary transactions endanger consumer rights when it comes to inadequate information disclosures, since consumers are placed in apposition where they have to *"consider whether and to what degree they are willing to have their personal data collected and used in exchange for receiving products or services."*[5]

25. In Colombia, the Consumer Protection Statute enshrines consumer's right to receive adequate information according to the terms of this law, to enable them to make informed choices.[6] To deliver adequate information, members of the production chain shall disclose *"complete, truthful, transparent, timely, verifiable, understandable, accurate and suitable information in respect of the products offered or put into circulation, as well as in respect of the risks which may arise from their consumption or use, the mechanisms for protecting their rights and the ways in which they may be exercised."* (Author's free translation).

26. In that sense, every time a company discloses inadequate information when it comes to the purposes for using their personal data, they would most likely be acting against the rights of the consumer, which in Colombia would be subject to an administrative investigation that could result in a monetary fine.

3.3. The use of unfair contract clauses in e-commerce transactions to collect large amount of data for unlawful purposes.

27. Misleading and unfair business practices that involve consumer data rights, also use online contracts as a fraudulent vehicle. In Colombia, consumers are entitled of the right to be protected from abusive clauses, under the terms of this same law.[7] Hence, contract clauses that inadequately inform or mislead consumers regarding their personal data might be infringing Colombian Consumer Protection Law.

28. Together and under the scope of ICPEN's activities, the SIC is currently participating in a joint action towards Apple Appstore and Google Appstore. This joint action consists in sending a written and official communication (supported and signed by about twenty consumer protection agencies from ICPEN), to ask the app store providers to ensure that apps can give relevant information on their main characteristics on personal data collection and usage before consumers download them. This, since App stores do not provide room for developers to inform consumers about data collection issues related to the use of the app.

29. Therefore, there is a lack of information on the essential/main characteristics of apps.

30. This activity is a preliminary approach to those large companies, without implying a withdrawal or absence of administrative actions by the authorities to enforce the law in

[4] (*Oecd.org*, 2020) <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf> accessed 6 May 2020.

[5] DSTI/CP(2018)17

[6] Article 1 of the Colombian Consumer Protection Statute –Law 1480 of 2011.

[7] Article 3 of the Colombian Consumer Protection Statute –Law 1480 of 2011.

their jurisdictions. Currently, this activity is still active, hopefully it results in a successful way to protect consumer data rights.

4. Role of Competition Advocacy

31. The SIC through the development of its competition advocacy role, recognised the importance of protecting data rights, when analysing an administrative act looking to reduce the risk of money laundering through payment postal services. The administrative act project, developed by the Ministry of Technologies of Information and Communication (henceforth, MINTIC), included the requirement of collecting consumer information, such as contact details, occupation, signature, and fingerprint. The Authority recommended the MINTIC to make payment postal service providers comply with the Data Protection Rules, defined by the Law 1581 of 2012[8].

32. In addition, the SIC has recognised the importance of lowering switching costs for the promotion of market competition in the industries of telecommunications, tolls for accessing road transport infrastructure and electronic invoicing. In 2017, the SIC analyzed the effects on economic competition of two administrative act projects, developed by the Ministry of Transport, looking to regulate the market for tolls to access road transport infrastructure. The first project regulated the legal, technical and financial conditions between intermediaries and operators of the national toll system, with the goal of facilitating nationwide transit of consumers subscribing contracts with individual intermediaries[9].

33. Regarding the first project and despite the expected positive effects on consumer welfare of the initiative, the SIC also highlighted the possible negative effects on competition of requiring all market participants to comply with the interoperability requirement. In this sense, the Authority claimed that the interoperability requirement might not had been sufficiently detailed on the project, and that the absence of precision regarding its application could result on an increase of market entry barriers. Resulting from the previous analysis, the SIC suggested the Ministry of Transport to detail the scope of the interoperability requirement in this or on subsequent administrative acts[10]. The Ministry of Transport, recognising the possible anticompetitive effects of the previous measure, developed an additional administrative act limiting the scope of the interoperability requirement, in line with the recommendations made by the SIC on its previous decision[11].

34. On a more recent decision, the Authority analysed the impact on market competition of an administrative act aiming to facilitate cell phone number portability and the economic compensation resulting from failures in calls [12]. The Authority welcomed the initiative based on the premise that the reduction of the maximum period in which

[8] Superintendencia de Industria y Comercio, Competition advocacy concept 13 - 171043 (2013). Consulted in http://normograma.info/sic/docs/cto_siyc_0171043_2013.htm

[9] Superintendencia de Industria y Comercio, Competition advocacy concept 17 - 192645 (2017). Consulted in http://normograma.info/sic/docs/cto_siyc_0192645_2017.htm

[10] *Id.*

[11] Superintendencia de Industria y Comercio, Competition advocacy concept 17 - 376636 (2017), Consulted in http://normograma.info/sic/docs/cto_siyc_0376636_2017.htm

[12] Superintendencia de Industria y Comercio, Competition advocacy concept 19 - 269527 (2019). Consulted in http://normograma.info/sic/docs/cto_siyc_0269527_2019.htm

communications companies were allowed to perform the number portability process would reduce transaction costs, allow consumers to take advantage of price reductions coming from other market competitors and, as a whole, increase market competition. In the path of arriving to this conclusion, the Authority took into consideration the recommendations made by the OECD claiming that facilitating number portability is a key instrument for increasing market competition on the fixed and mobile telephony industry [13].

35. Finally, the SIC studied an administrative act project, created by the Ministry of Trade, Industry and Tourism (henceforth, MINCIT), aiming to regulate the development of electronic invoicing. Regarding this matter, the SIC recognised the importance of setting requirements for allowing companies to develop this process adequately; however, the Authority also highlighted the possible anticompetitive effects that could result from the definition of unnecessary high standards that could disincentivise market entry or that could difficult competition by existing participants. Additionally, the Authority suggested the MINCIT to design the legal framework in a way that would increase competition on the factoring market through the lowering of consumers' switching costs between suppliers.[14]

36. Overall, the SIC has recognised the role played by switching costs on different markets in relation to the promotion of market competition and has supported and promoted regulatory modifications on the telecommunications and tolls for accessing road transport infrastructure markets in this regard.

5. Final remark

37. The Superintendence of Industry and Commerce has enforced and advised on the protection of data rights of consumers. Through decisions from its Deputy Superintendences and involvement in international venues, the SIC has recognized the importance of guaranteeing consumers access to and control of their data. Also, the SIC has examined, among others, the potential effects of the abuse of targeted advertisement over consumers decision-making; unfair contract clauses in e-commerce transactions to collect large amounts of data; unfair and deceptive practices in connection with the collection, use and disclosure of personal data to third parties and the competition impacts of data portability.

[13] *Id.*

[14] Superintendencia de Industria y Comercio, Competition advocacy concept 19 - 256945 (2019). Consulted in http://normograma.info/sic/docs/cto_siyc_0256945_2019.htm