

**DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE**

The intersection between competition and data privacy – Note by Costa Rica

13 June 2024

This document reproduces a written contribution from Costa Rica submitted for Item 8 of the 143rd OECD Competition Committee meeting on 12-14 June 2024.

More documents related to this discussion can be found at
www.oecd.org/competition/intersection-between-competition-and-data-privacy.htm

Antonio CAPOBIANCO
Antonio.Capobianco@oecd.org, +(33-1) 45 24 98 08

JT03543603

Costa Rica

1. Introduction

1. The intersection between competition and privacy has emerged as a rapidly evolving area of importance within the contemporary regulatory landscape. In a digitized world where massive data collection is commonplace, the inevitable question arises: how can competition authorities and privacy regulators collaborate effectively to address the challenges posed by this convergence? This essay aims to explore this issue, focusing on the joint initiative of the OECD Competition Committee and the Working Party on Data Governance and Privacy to examine the interactions between these two policy domains.

2. Data Protection in Costa Rica

2. In Costa Rica, the protection of personal data is regulated primarily by the provisions contained in the Law for the Protection of the Individual against the Processing of their Personal Data, Law 8968. This law aims to guarantee respect for the fundamental right of individuals to informational self-determination, as well as the provisions of the General Telecommunications Law, Law 8642, regarding the privacy of communications. This regulation stems from the provisions of Article 24 of the Political Constitution, regarding the right to privacy, freedom, and the secrecy of communications.

3. Law 8968 dates back to 2011, and through this law, the Agency for the Protection of the Personal Data of the Inhabitants (PRODHAB- acronyms in Spanish) was created. This regulatory framework has not undergone substantive reforms to date, and therefore falls short in terms of the necessary provisions to regulate data protection issues in a digital environment.

4. In particular, the OECD Committee on Digital Economy Policy recommended a series of measures to Costa Rica regarding the protection of personal data, including: i) ensuring that PRODHAB's privacy strategy reflects a coordinated approach among different government bodies; ii) developing and implementing monitoring and evaluation methodologies for data protection activities to underpin policies; and iii) adopting appropriate measures to facilitate cross-border cooperation in privacy law enforcement.

5. This has led to considering the need for a new Personal Data Protection Law in the country that addresses current needs in the field. Currently, two draft laws aimed at modernizing the regulatory framework for personal data protection are in the legislative pipeline.

6. The first is the Comprehensive Reform Bill to the law for the protection of the individual against the processing of their personal data, file 22.388, which seeks to reform Law 8968. The second is the Personal Data Protection Bill, file 23.097, which aims to establish a new regulatory framework in the field, providing a complete rethinking of the regulatory system in the field. Both draft laws are inspired by the General Data Protection Regulation (GDPR) number 2016/679, which came into effect in the European Union on May 25, 2018.

7. Among other relevant aspects, these draft laws address elements that seek to provide the country with tools in the field of personal data protection to address the challenges of a data-based economy, as well as to reconcile the importance of cross-border

flows of personal data with broad guarantees for compliance with data protection of citizens in a technological uncertain environment.

8. Both draft laws develop the rights of the data subject regarding their personal data in terms of access, rectification, cancellation, and opposition, including the figure of the right to data portability. Likewise, they regulate international transfers of personal data, proactive measures in the processing of personal data, including figures such as privacy by design and privacy by default, and self-regulation mechanisms. The data protection authority is strengthened, and rules for data transfer between public institutions are introduced, among other elements.

3. Privacy Considerations in Competition Cases

9. One key issue raised is whether competition authorities are adequately taking into account privacy considerations in their cases. Traditionally, antitrust investigations have focused on issues such as the restriction of competition and abuse of dominant position. However, in the current digital context, data collection and use can play a fundamental role in determining anticompetitive effects.

10. As companies collect and use large amounts of data to develop innovative products and services, concerns arise about potential negative effects on competition. Privacy regulators must be mindful of how data collection and usage practices can impact competition in the market and therefore consider these concerns in their data protection work.

11. In the digital age, where massive data collection is ubiquitous, the question arises of whether data concentration in the hands of a few dominant companies can undermine competition by creating barriers to entry for new competitors. This relates to the idea that the accumulation of data by large companies may give them an unfair competitive advantage, raising questions about whether privacy can be considered a facet of antitrust concerns.

12. In a merger or acquisition, it is important to assess whether the combination of data from the companies involved in the transaction could result in an increase in market power that may be detrimental to competition. In such cases, protecting users' privacy may be a relevant factor to consider in evaluating the competitive effects of the transaction.

13. In relation to the draft laws currently under consideration in the Costa Rican legislative process, it is considered indispensable to ensure that upon the issuance of a new legal framework regarding the protection of personal data, the country adopts a coordinated approach among different government bodies. In this regard, the OECD has stated: "[...] a rigid separation between the scope of competition, consumer protection, and data protection authorities is highly likely not to lead to optimal outcomes, in terms of consumer welfare and protection. For this reason, it may be that all three policy areas need to be applied in parallel [...]".

14. It has been assessed that the proposed regulations establish administrative requirements that economic agents must comply with regarding the safeguarding and processing of personal data information, and that compliance with such requirements may entail associated costs for implementation, which warrants special care. It is therefore recommended that the draft laws have appropriate compliance costs that do not create barriers to entry, thus allowing the objectives of personal data protection to be achieved in a way that minimizes their potential impact on competition.

15. One positive aspect is that the draft laws do not specify the specific form (technical standards or norms) for compliance with these requirements. This opens up space for agents to determine the most convenient way to comply, thus reducing implementation costs. Additionally, in the matter of recording treatment activities, this obligation is eliminated for small businesses, further reducing costs for smaller enterprises. This is appropriate to ensure that competition prevails, as these implementation costs can disproportionately harm smaller companies.

16. Regarding Bill 23.097, which addresses the issue of consent, it is also highlighted that mechanisms for obtaining express consent (opt-in), as proposed in the bill, may disproportionately affect small and new businesses, potentially impacting market competition. It is recognized that this is more likely to occur when compliance costs are largely fixed (regardless of company size), making them more burdensome for smaller companies compared to larger ones, thus generating economies of scale and scope to obtain consumer consent.

17. It has also been noted that to the extent that privacy and data protection laws make it difficult for companies to acquire and use data from consumers they do not themselves have, this could strengthen holders who already have consent to collect and use large amounts of consumer data.

18. Regarding data communication or transfer issues, it has been pointed out that data portability mechanisms contribute significantly to addressing concerns that may arise from data transfer between market agents.

19. The proposals establish the use of data portability mechanisms, and it has been recommended that they not be burdensome to the extent that they limit the ability of economic agents to compete in the market, thus ensuring that the implementation of this mechanism is appropriately designed and does not negatively impact competition.

20. Finally, it has been recommended that the data protection agency be empowered to enter into cooperation agreements with other national authorities to ensure adequate coordination and the fulfillment of public purposes for the benefit of consumers.

21. In the same line, within the context of analyzing the Draft Law on Remunerated Non-Collective Transportation of Persons and Digital Platforms, it offers a crucial perspective on how the functionality requirements established for technological platforms can influence market competition dynamics. The criteria issued considered the impact of such requirements from the perspective of competition law, highlighting both the potential benefits and limitations that could arise from these regulations.

22. Functionality requirements focus on aspects such as computer security and information privacy and have the potential to affect competition in the technological platform market in various ways.

23. On one hand, these regulations can foster competition by establishing minimum standards that all platforms must meet to operate in the market. By reducing entry barriers related to data security and privacy, these regulations could promote the entry of new competitors, increasing competition and potentially benefiting consumers through greater variety of options and lower prices.

24. On the other hand, these regulations can also safeguard competition by ensuring that all technological platforms compete on equal terms in terms of computer security and information privacy. This could prevent anticompetitive practices related to data manipulation or exploitation of security vulnerabilities by dominant companies, ensuring a level playing field for all market participants.

25. However, it is crucial to consider that these regulations may also have adverse effects on competition. For example, they could create additional barriers to entry and expansion in the market, especially for smaller or newer companies that may struggle to comply with the established requirements. This could limit innovation and restrict competition, which in turn could harm consumers by reducing the diversity of products and services available.

26. While these regulations have the potential to promote healthy competition by ensuring a minimum level of security and privacy for all market participants, it is essential to strike an appropriate balance to avoid creating unnecessary barriers to entry and expansion in the market. Ultimately, the success of these regulations will depend on how they adapt to the changing dynamics of the market and are effectively implemented to ensure a fair and dynamic competitive environment in the technological platform sector.

4. Synergies and Challenges in Cooperation

27. While there is a clear imperative for competition authorities and privacy regulators to collaborate more closely, significant challenges exist in implementing this cooperation. Differences in regulatory frameworks, methodological approaches, and institutional cultures can hinder the effective integration of privacy considerations into the realm of competition and vice versa. However, the resulting synergies from this cooperation can lead to more coherent and effective regulation that comprehensively addresses the challenges posed by the intersection of competition and privacy.

28. There are areas where synergies between competition and privacy can be identified, such as consumer protection and the promotion of innovation. On the other hand, there are also significant challenges, such as reconciling the objectives of competition and privacy protection in situations where they may conflict.

29. In some cases, privacy provisions may limit companies' ability to share data with third parties, which could hinder competition in the market. On the other hand, the anticompetitive practices of some companies may involve the unauthorized collection and misuse of consumers' personal data, which may raise additional concerns in terms of data protection. For example, excessive regulations imposing unnecessary administrative burdens on companies can hinder the entry of new competitors and limit innovation in the market.

30. In the context of data protection, regulations imposing overly strict restrictions on the processing of personal data may hinder companies' ability to develop innovative products and services that rely on data analysis. This can negatively affect the competitiveness of companies in the global market and reduce their ability to compete with other companies operating in jurisdictions with more flexible data protection regulations.

5. Conclusions

31. In summary, the interaction between competition policy and data protection in Costa Rica is a complex issue that requires a balanced approach taking into account the interests of both competition and privacy. While significant progress has been made in regulating both areas, there are still important challenges in terms of reconciling these sometimes-divergent objectives. Cooperation among competition and data protection regulators, as well as greater harmonization of laws and regulations in these areas, can be

key to addressing these challenges and promoting a competitive business environment that respects privacy in Costa Rica.