Organisation for Economic Co-operation and Development

DAF/COMP/WD(2024)22

Unclassified

English - Or. English

14 May 2024

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

The intersection between competition and data privacy – Note by Brazil

13 June 2024

This document reproduces a written contribution from Brazil 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

JT03543600

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Brazil[1]

1. Introduction

1. According to Adel (2022[1]), "the revolution of industry 5.0 means that humans and machines are working together, improving the efficiency of industrial production. Human workers and universal robots are boosting the productivity of the manufacturing industry". Therefore, it is possible to observe an intelligent industry, with convergence of advanced technologies such as artificial intelligence, big data, internet of things (IoT), and robotics into industrial processes. (MALIK and ABBAS, 2024[2]).

2. As automation and robotics permeate industry at an accelerated pace, industrial standards and interoperability become salient concepts within Competition Law, in a society interconnected by intricate systems. (HOVENKAMP, 2023[3]). Antitrust legislation is instrumental in thwarting the manipulation of standard-setting protocols or the enforcement of exclusive standards that impede fair competition. In the sphere of standardization, cybersecurity plays a pivotal role in ensuring the strengthening of interoperable systems against cyber threats, thereby safeguarding their security and resilience.

3. In industry 5.0, data is sometimes referred to as the new currency (MAKRIDIS and THAYER, 2023[4]; NUNWICK, 2023[5]; EGGERS, HAMILL and ALI, 2013[6]). In this scenario, companies collect vast amounts of data from various sources including IoT devices, customer interactions, and supply chain operations.

4. In today's dynamic environment of ever-changing and manifold consumer behaviors, it is paramount for companies to harness these patterns to be competitive (BAO et al., 2022[7]). By constructing user profiles and implementing a classification framework, they can delineate the intricate relationship between consumers and products, thereby mirroring the desires and inclinations of consumers (ZHANG, 2023[8]).

5. Moreover, these technologies that intensely and automatically gather personal data can be utilized to maximize profits by optimizing company´s prices.

> *"Imagine the pre-sales process of a car insurance company. The core issue is to optimize the price of the premium it charges to buyers. In the IoT era, insurers can request their customers to use a mobile app or another type of telematics (geospatial application) to collect information, such as speed, distance, and time of day, in order to price the premium more accurately. This means that premiums are lowest for responsible drivers.*
>
> *(...)*
>
> *Another interesting example from car insurance is the Admiral's FirstCarQuote.*[2] *It is aimed at young drivers who are going to have their first car and have no history of driving. Because of the lack of track record, the insurance company faces a typical problem of adverse selection: it is very difficult to differentiate a responsible*

[1] This document was written by Alexandre Cordeiro Macedo, President of CADE, and Ricardo Medeiros de Castro, Head of the Technical Advisory Unit to the Office of the President of CADE

[2] See https://www.wired.co.uk/article/admiral-facebook-policy. Accessed on Feb, 15th, 2024.

> *driver from one who is more likely to cause a claim. The app requires potential insurance buyers to login using their Facebook profile. After that, an artificial intelligence algorithm scans the user's past likes and posts on Facebook to estimate a behavioral measure of how conscientious, responsible and organized the user is. This is a typical example of an IoT environment due to the interconnection of two platforms in order to acquire behavioral data."*
>
> (NUNES and GONÇALVES, 2017[9])

6. This may be considered intrusive for some consumers. Also, this illustrates how market player discriminates consumers in a granular level through the use of new technologies.[3]

7. Competition authorities, relying on traditional demand measurement models, merger simulations, and analysis of the effects of anticompetitive conduct, need to keep pace with the evolving techniques through which companies actually make decisions, price discriminate against consumers, and exercise their market power.

8. At times, however, the pursuit of extensive data collection methodologies may exact a toll on the erosion of individual privacy safeguards. Therefore, it is pertinent to debate the extent to which Competition Law intersects, to some degree, with discussions concerning privacy protection. That is the purpose of this article.

9. So, the current investigation delves into disparate viewpoints regarding how Competition Law and Personal Data Protection Law can interact with one another in merger analyses.

10. The structure of the article is quite straightforward. After a brief introduction, the intention is to present the arguments of some authors who are in favor and others who are against the inclusion of privacy protection issues within the scope of merger and acquisition analyses. Subsequently, the study will seek to present how CADE has positioned itself in this debate.

2. Privacy concerns in merger analyses

11. In Brazil, the right to privacy is duly recognized as having constitutional status. In this regard, Article 5, X of the Brazilian Constitution states that: "privacy, private life, honor, and image of individuals are inviolable." Furthermore, Article 5, LXXIX of the Constitution is even more specific, stipulating that "the right to the protection of personal data, including in digital media, is guaranteed by law." On the other hand, free competition is also elevated to a constitutional principle of significant stature (see Article 170, IV and Article 173 § 4º of the Constitution).

12. At the same time, Competition Law and Privacy Protection Law have some intersections. For example, some strong players in the market secretly collected

[3] According to Coll (2015[28]), there are several principles that could assist various citizens in gaining more control over their own data. Transparency, for instance, could help consumers understand which companies possess and utilize their respective data. Many individuals experience a sense of disempowerment regarding their data control (AU10TIX, 2022[29]), due to the surreptitious collection of their personal information via cookies, sometimes without their prior knowledge. Additionally, some companies retain (and sometimes even sell) such data without the user's explicit authorization. A study conducted in the US in 2009 showed that 87% of participants did not wish to receive tracking-based advertisements (MAYER and MITCHELL, 2012[30]; TUROW et al., 2009[31]). Another issue raised by Coll (2015[28]) concerns "access": that is, the possibility for citizens to view and retrieve their own data that is automatically collected by companies in the digital environment. This type of concern is expressed by the Midata program (REINO UNIDO, 2011[32]) and the MyData initiative (POIKOLA et al., 2020[33]).

information of consumers, through automatic means.[4] This could represent a breach of Privacy Law. However, some argue that collection and possession of data may generate market power, especially if other competitors cannot reasonably collect, replicate, purchase or substitute such data (CMA, 2015[10]; RISTANIEMI and PUUTIO, 2016[11]). In this sense, Yan Carriere Swallow and Vikram Haksar (2019[12]) argued that:

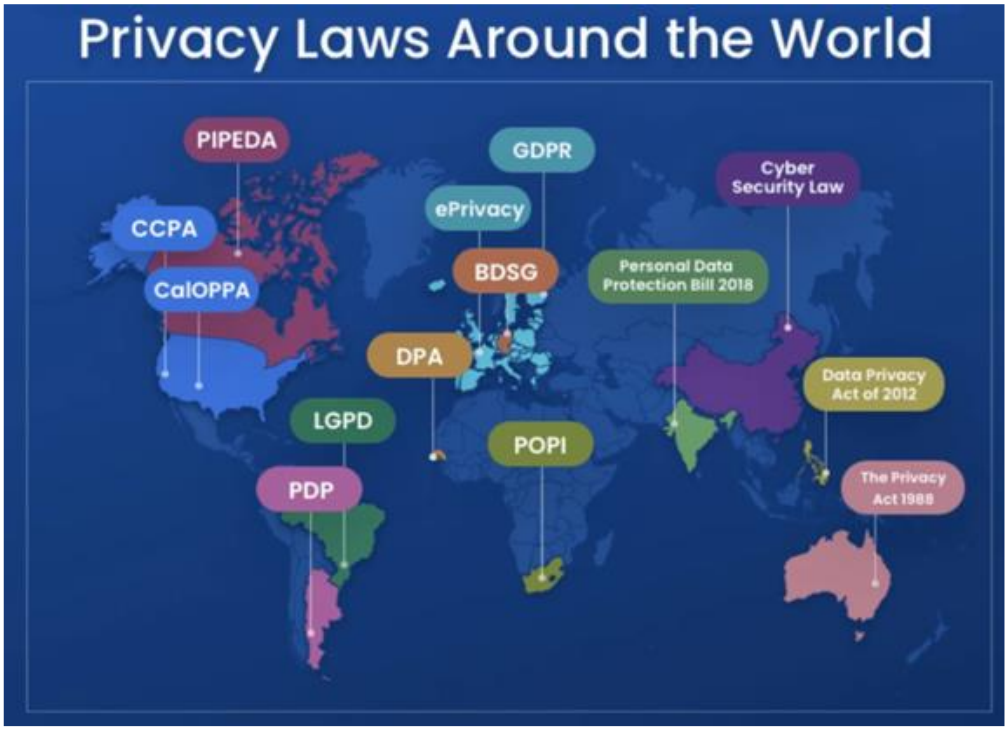
> *" If a data collector enjoys market power, then obtaining granular information on their clients may enable them to extract considerable rents through the implementation of price discrimination strategies. Data may also be a source of market power if a stockpile of data acts as a barrier to entry that deters competition."*

13. In Brazil, with Constitutional Amendment 115 and, considering Law No. 13,709, dated August 14, 2018, amended by Provisional Measure No. 869, dated December 27, 2018, subsequently converted into Law No. 13,853/2019, the regulation of the matter was established through a legislation known as the General Data Protection Law (LGPD), which is responsible for creating the National Data Protection Authority (ANPD).

14. Similar to the LGPD, there are several other privacy protection laws around the world.

[4] According to Gabrielle B. S. Sarlet and Daniel P. Rodrigues (2022, p. 222[34]), Amazon, a strong player in the market, at least until July 2019, secretly collected voice recordings of minors without the consent or knowledge of their parents. On the other hand, the company reached an agreement with US authorities, resulting in a $30 million settlement (REUTERS, 2023[35]), to resolve the case. In the European context, the General Data Protection Regulation (GDPR) represents the legislation for the protection of personal data in that jurisdiction, having been drafted in 2016. The GDPR came into force in 2018, replacing the old Directive 95/46/EC (BOIT, 2022, p. 29[36]) . According to the Data Privacy Manager blog (2023[37]), there have been a series of fines imposed on major companies in the digital market based on this legislation, such as the €1.2 billion fine by the Irish Data Protection Commission (DPC) against the US company Meta for improper transfers of consumer data from Europe to the United States. Another case concerned the €405 million fine against Meta Ireland regarding the legality of processing personal data of children.

Figure 1. Privacy Laws Around the world



Source: https://gpotcenter.org/data-privacy-laws/ Retrieved: 16 Feb 2024

15. Although the ANPD is the competent regulatory agency to deal with issues related to personal data protection, there are those who advocate for an integration of Competition Law with privacy protection norms. Others, however, believe that this relationship should not be organic, but merely functional. In the next sections, both theories will be presented.

2.1. Theory in favor of considering Privacy in merger analysis

16. Bundeskartellamt of Germany and the French Competition Authority, Autorité de la Concurrence, in a document entitled "Competition Law and Data" (FRANCE and GERMANY, 2016[13]) , pointed out that the possession and use of data are increasingly considered within competition law itself. Especially, in the Judgment of the European Court of Justice, in case C-252/21, involving Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, and Facebook Deutschland GmbH, the question was debated as to whether Meta could aggregate data obtained within and outside the social network "Facebook" without consumers being able to agree to such aggregation or whether such a procedure could represent some kind of abuse of market power (and whether the Competition Authority would have competence to address this issue).

17. On that occasion, the European Court of Justice clarified that national competition authorities may oversee, in the exercise of their powers, whether the processing of personal data complies with the requirements established in Data Protection Legislation.

18. Joseph Farrel (2012, pp. 251-252[14]) claims that a considerable number of individuals perceive surveillance and tracking as discomforting. The degree to which consumers prioritize privacy varies among individuals, and the discomfort associated with surveillance varies across different circumstances. However, consumers also care about

privacy in a more instrumental way. For instance, loss of privacy could identify a consumer as having a high willingness to pay for something, which can lead to being charged higher prices.

19. Also, Rober Lande (2008[15]) mentioned that, in 2007, the Federal Trade Commission (FTC) analyzed the Google/DoubleClick merger to determine if it posed antitrust concerns. While the majority of the Commission concluded that the merger wouldn't harm consumer privacy, one Commissioner dissented, expressing concerns about potential negative impacts on privacy. According to Robert Lande, Antitrust laws are not solely concerned with prices; they aim to safeguard consumer choice in various forms, including price, variety, innovation, quality, and privacy protection. This broader perspective, according to Lande, acknowledges that consumer welfare encompasses more than just price, including the preservation of privacy rights in the face of corporate mergers and market consolidation.

20. Using a similar line of thought, Andressa Fidelis (2017[16]) argued that data-driven mergers represent transactions geared towards acquiring, amalgamating, and capitalizing on vast quantities of commercially valuable data sourced from diverse origins and formats. According to Fidelis, these mergers, prevalent in digital markets, such as e-commerce, social networks, search engines, and online advertising, are exemplified by notable deals like Verizon/Yahoo! (2016), Microsoft/LinkedIn (2016), Facebook/WhatsApp (2014), and Google/DoubleClick (2008), among others. Leveraging advancements in artificial intelligence, data mining, and machine learning, these transactions enable data analysis for insights that can drive down product and process innovation costs. According to Fidelis, consumers' data lies at the heart of these business models and significantly contributes to the market dominance of industry giants like Apple, Alphabet, Microsoft, Amazon, and Facebook.

21. Fidelis believes that the nature of data lends itself to long-term dominance, raising concerns about the entrenchment of data-driven platforms at the expense of innovation, consumer welfare, and democracy. Successful data-driven platforms leverage their established user base to collect, store, and process large volumes of real-time data, allowing for precise analysis of user interests, sentiments, influence, and behavior.

22. Fidelis claims that, in the realm of mergers, both the European Commission (EC) and the Federal Trade Commission (FTC) have approved the Google/DoubleClick merger without properly addressing privacy concerns, except for a dissenting statement from former FTC Commissioner Pamela Jones Harbour, who considered privacy issues as 'cognizable.' The EC, in the Facebook/WhatsApp case, dismissed privacy concerns as beyond the scope of EU competition law, a stance echoed by the European Court of Justice in the Asnef-Equifax case. However, given that privacy can impact economic efficiency and long-term consumer welfare, Fidelis considers privacy, as a dimension of quality competition, that should be part of antitrust analysis, as lower quality can be as harmful to consumer welfare as higher prices.

23. The author states that the merger between Facebook and WhatsApp was responsible for decreasing the level of privacy protection. According to her, the merger between Facebook and WhatsApp brought together two consumer communication apps with different approaches to privacy protection. WhatsApp prioritized message encryption, while Facebook Messenger extensively collected user data for advertising purposes, even storing deleted messages on its servers. This privacy discrepancy led many users to favor WhatsApp over Messenger. Consequently, Competition Authorities approved the merger, believing the two services were not direct competitors and that consumers still had ample alternative choices for communication apps. However, two years later, WhatsApp announced it would share user information with Facebook, contrary to earlier assurances

given in merger procedures. So, by Fidelis' point of view, by acquiring WhatsApp, Facebook potentially limited consumer privacy choices and disrupted the competitive balance.

24. In light of this theoretical framework, proponents assert the necessity for heightened competition regulation, advocating for a cohesive integration between the realms of personal data protection and Competition Law. Nevertheless, it is imperative to also consider the perspective of those harboring greater skepticism towards this proposed approach.

2.2. Theory against of considering Privacy in merger analysis.

25. As mentioned by Bhattacharya and Buiten (2018[17]), many proponents advocating for the utilization of competition law to address privacy concerns express apprehension regarding the mergers of data-rich corporations, which amalgamate previously segregated reservoirs of consumer information. They argue that the amalgamation of data alone raises privacy concerns and needs some intervention.

26. However, according to Bhattacharya and Buiten, the consolidation of data across business platforms frequently engenders substantial efficiencies and enhances consumer welfare. The collection and utilization of consumer data online has the potential to enhance services, enabling firms to furnish superior services at reduced prices or free of charge. Also, they claim that altering the conventional antitrust analysis to accommodate subjective assessments of harm to consumer privacy may generate differential treatment among mergers, with outcomes contingent upon subjective perceptions of privacy.

27. More central to the argument presented by Bhattacharya and Buiten (2018, pp. 8-9[17]) is the fact that they do not see Big Data as a necessary entry barrier or any form of essential input for disruptive businesses.

28. Using the same kind of logic, James Cooper (2013, p. 16[18]) argues that unlike a conspiracy to fix prices, data collection and its use do not represent any conduct that directly harms competition. Rather, using antitrust to limit the collection and use of consumer data would decrease the amount of marketplace information available to consumers, rendering markets less efficient.

29. James Cooper (2013, p. 9[18]) also mentions that, for some consumers, the notion of being tracked online or having their emails scrutinized by Google (or other enterprises) may hold little significance, especially if they derive considerable utility from the convenience of streamlined searching and the delivery of highly relevant advertisements. Conversely, there exists a segment of individuals who harbor a strong aversion towards targeted ads and experience a disquieting sensation upon realizing that their search and browsing histories are archived across multiple servers. For these individuals, the accumulation of data may represent a discernible diminishment in the overall quality of their online experiences.

30. Upon acknowledging the diversity among consumers, the decisions made by specific players in digital markets to intensify data collection efforts, according to Cooper, do not necessarily mean a manifestation of market power, in the sense that the ultimate result of this approach is ambiguous in terms of effects.

31. Maureen Ohlhausen and Alexander Okuliar (2015[19]) consider that while antitrust laws possess the authority to halt transactions, they fall short as a comprehensive solution for privacy concerns. Blocking a merger between two entities with substantial datasets wouldn't eradicate the issue entirely. Instead, it's plausible that the involved parties would be motivated to devise alternative arrangements, such as licensing agreements or the

transfer of data to third-party repositories, thus circumventing antitrust scrutiny. Additionally, they claim that antitrust authorities are ill-equipped to address privacy issues stemming from the prolonged aggregation of data by a single entity. Conversely, Ohlhausen and Okuliar (2015[19]) argue that consumer protection laws offer more robust mechanisms for addressing privacy breaches.

32. Ohlhausen and Okuliar (2015[19]) considered that the concerns regarding privacy stemming from the amalgamation of datasets do not automatically justify intervention under competition law. The central issue when assessing such mergers lies in determining whether the data involved possess sufficient 'uniqueness' to erect barriers to entry, thereby hindering competition. Personal data lacks the typical attributes necessary to constitute a barrier to entry. It is a non-essential input, widely available, and obtainable from various sources. Furthermore, the acquisition of big data is relatively straightforward, given that the production and distribution costs are nearly negligible. Data are non-exclusive and non-rivalrous, as multiple sources exist, and no single provider holds exclusive rights over user data. Additionally, many consumers engage in 'multi-homing,' utilizing similar services from different providers and sharing their personal data accordingly.

33. Moreover, the value of data depreciates over time. Recent achievements by innovative, disruptive startups serve as evidence that entry barriers in data-rich markets are not inherently insurmountable. These startups swiftly emerged and displaced established firms, despite the latter possessing more extensive data resources. Examples include Airbnb, Uber, Snapchat, and Tinder, all of which attained rapid success by introducing innovative products that catered to consumer needs, even in markets with established network effects. (OHLHAUSEN and OKULIAR, 2015[19])

34. Therefore, it is possible to see a very clear argument from some authors that Competition Law should not interfere in the assessment of issues involving privacy.

2.3. Brazilian perspective

35. With the aim of accurately gauging what CADE has understood regarding this matter, the present study employed the methodology of “term counting” in official documents to assess the intensity of discourse and arguments presented within the scope of the Brazilian competition authority. The counting of terms, such as citation analysis, has been used as a methodology in other scientific works, such as Cronin (1984[20]), Feist (1997[21]) and suggested in Law by Posner (2000).

36. So, the present study conducted an exploratory analysis on the document collection called the Electronic Document System (SEI). In this system, access is available to all CADE’s internal documents, petitions, and CADE´s decisions in specific cases. It is important to emphasize that there is a possibility for the search system to not fully capture all the relevant documents, due to the specificity of the search itself or the fact that new documents can be included in CADE´s database.

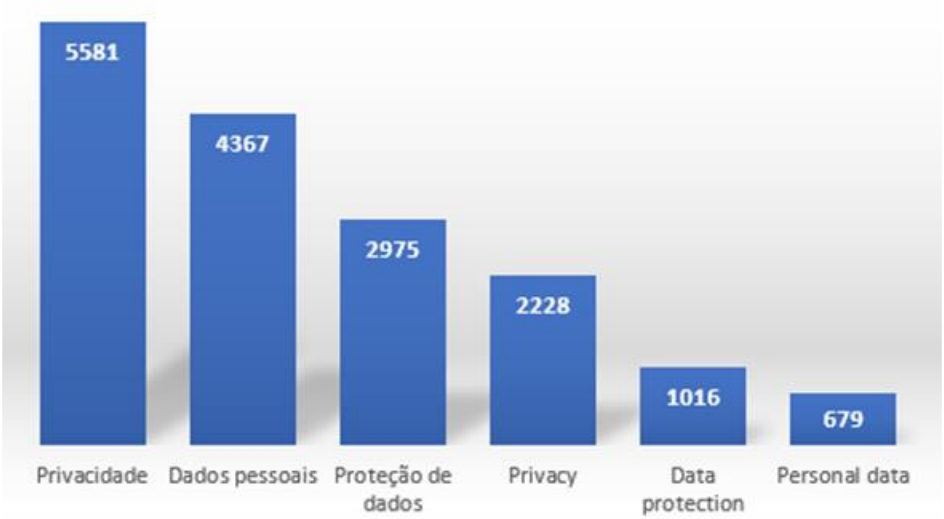
37. Through this procedure, the goal was to measure the frequency of times certain words related to Data Protection Law and the Right to Privacy were referenced.

38. The following terms were selected in our study:

- Privacidade (or “Privacy”)
- Dados pessoais (or “Personal data”)
- Proteção de dados (or “data protection”)

39. In the chart below, it is possible to identify the quantity of citations for each of the aforementioned terms:

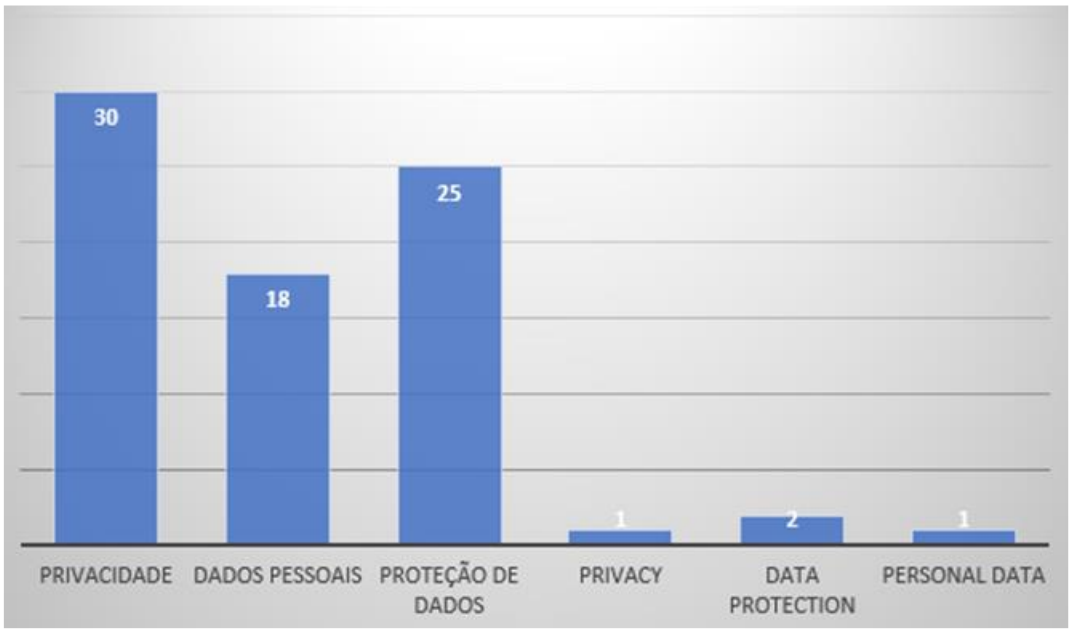
Figure 2. Number of documents referencing terms related to privacy in CADE's electronic system (SEI)



40. On the other hand, these results do not necessarily pertain to the assessment of whether "privacy" should be considered as a value to be protected in terms of mergers and acquisitions or administrative processes. In reality, what is observed is that CADE also needs to comply with the General Data Protection Law, as well as frequently deciding whether a certain type of document is restricted from access (or whether the publicity of the document may entail some form of sensitive, personal data, or information that violates the privacy of the entity that provided information to CADE).

41. Therefore, to conduct a more detailed evaluation, a filter was applied to select only the votes or decisions that made explicit reference to such terms. Here are the results obtained:

Figure 3. Number of decisions referencing terms related to privacy in CADE's electronic system (SEI)



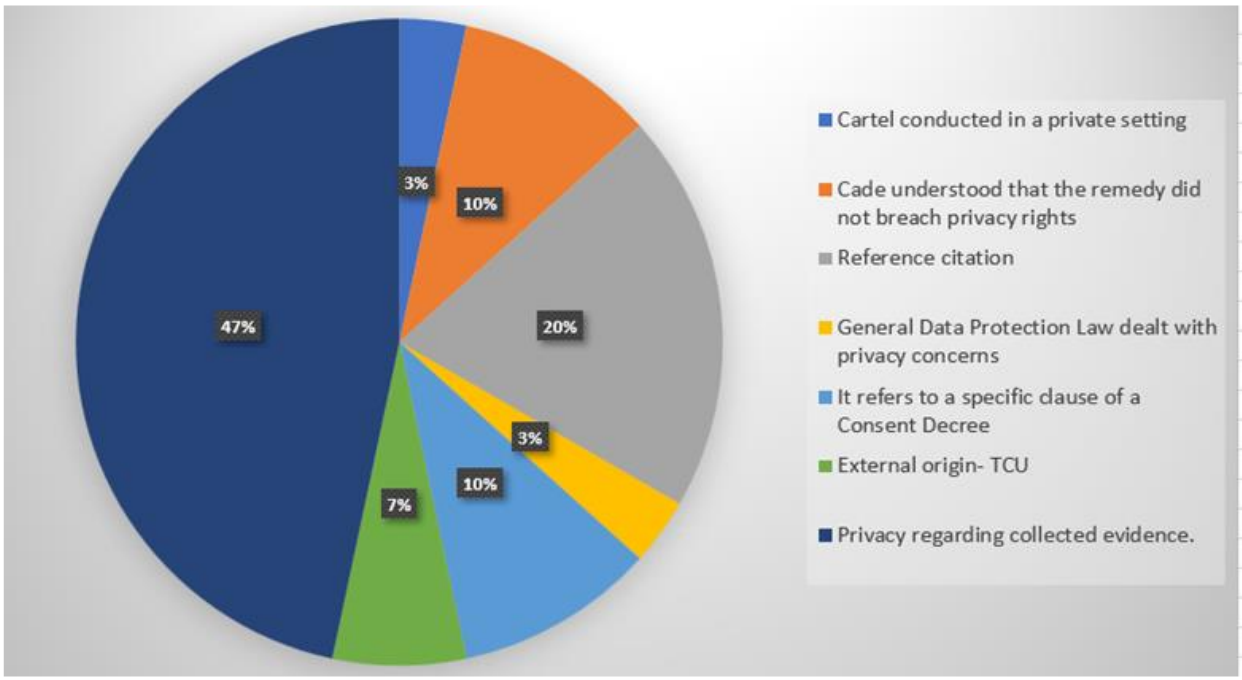
42. The problem, however, is that even controlling for "votes" or "decisions" this search is not restricted only to CADE´s commissioners decisions. There are some votes or decisions in SEI that are from other sources (such as Judicial Tribunals).

43. However, when considering the 30 decisions that mentioned the term "Privacidade", none of them made explicit reference to it as a value protected or protectable by Competition Law. On the contrary, the understanding went in the opposite direction, as follows.

Table 1. Documents presenting CADE or other courts' decisions available in CADE's electronic system (SEI)

Case	Document	Reference to Privacy as a value to be protected in Antitrust?	Explanation
08012.008850/2008-94	83683	No	Cartel conducted in a private setting
08012.011142/2006-79	92323	No	Cade understood that the remedy did not breach privacy rights
08700.000384/2022-07	1013975	No	Cade understood that the remedy did not breach privacy rights
08700.002792/2016-47	263825	No	Cade understood that the remedy did not breach privacy rights
08012.010483/2011-94	632170	No	Reference citation
08700.003075/2019-85	628675	No	Reference citation
08700.003194/2019-38	631140	No	Reference citation
08700.003542/2019-77	636406	No	Reference citation
08700.010872/2014-04	631208	No	Reference citation
08700.004655/2021-12	951131	No	Reference citation
08700.001813/2021-74	891385	No	General Data Protection Law dealt with privacy concerns
08700.002488/2022-48	1296318	No	It refers to a specific clause of a Consent Decree
08700.004255/2023-61	1249661	No	It refers to a specific clause of a Consent Decree
08700.009905/2022-83	1250888	No	It refers to a specific clause of a Consent Decree
08700.002652/2021-36	1078145	No	External origin- TCU
08700.001202/2021-26	1086155	No	External origin - TCU
08012.002568/2005-51	281059	No	Privacy regarding collected evidence.
08012.003321/2004-71	188198	No	Privacy regarding collected evidence.
08012.008215/2006-45	475969	No	Privacy regarding collected evidence.
08012.008855/2003-11	43120	No	Privacy regarding collected evidence.
08012.010187/2004-64	85185	No	Privacy regarding collected evidence.
08012.010932/2007-18	27924	No	Privacy regarding collected evidence.
08700.000729/2016-76	447404	No	Privacy regarding collected evidence.
08700.000738/2016-67	447413	No	Privacy regarding collected evidence.
08700.000739/2016-10	447416	No	Privacy regarding collected evidence.
08700.001174/2018-41	446967	No	Privacy regarding collected evidence.
08700.001885/2017-35	909587	No	Privacy regarding collected evidence.
08700.002585/2021-50	907793	No	Privacy regarding collected evidence.
08700.002882/2021-03	912401	No	Privacy regarding collected evidence.
08700.011474/2014-05	25131	No	Privacy regarding collected evidence.

Figure 4. Documents presenting CADE or other courts' decisions available in CADE's electronic system (SEI)



44. As illustrated, 47% of the decisions pertained to evidentiary issues: whether the collected evidence could be used in CADE's proceedings, considering due process and the protection of privacy of the parties in a search and seizure procedure. Therefore, the issue regarding Privacy as a potential objective to be pursued by Antitrust was not addressed.

45. In one specific case, however, CADE analyzed a merger between Magalu Pagamentos Ltda. ("Magalu Pagamentos") and Hub Prepaid Participações S.A. ("Hub") which was unconditionally cleared by the Office of the General Superintendent on March 17, 2021. Mercadopago.com Representações Ltda. ("Mercado Pago"), as an Interested Third Party, contested the decision. Mercado Pago argued that the operation involved competitive issues in the data-driven digital economy, emphasizing the value of big data in this context. It was alleged that Magalu Pagamentos could use Hub's banking database to gain undue competitive advantages, especially related to Mercado Pago's customers. CADE, in its decision, considered that this merger should be unconditionally cleared, as commitments and safeguards were adopted by the parties involved. Regarding privacy, the decision took into account the General Data Protection Law (LGPD), which regulates the processing of personal data, ensuring respect for privacy. The provisions of the LGPD, along with other contractual and regulatory obligations, were considered sufficient to prevent any undue transfer of customer data to Magalu Pagamentos and to discourage any inappropriate behavior by Hub.

46. However, CADE did not agree with the thesis that Privacy concerns could be adjudicated in an antitrust analysis, but only that LGPD was enough to deal with these problems.

47. There was another interesting debate in merger 08700.009905/2022-83, involving the creation of a joint venture in the Netherlands among several companies (SustainIt Pte Ltd, Cargill Incorporated, Louis Dreyfus Company Participations B.V., and ADM International SARL), aiming to develop a B2B software platform to track sustainability metrics in the food and agricultural supply chain, such as CO_2 emissions. The platform

collects and processes information on the sector's sustainable performance. CADE approved the operation, with a consent decree.

48. An issue involved in the debate was whether the data privacy of each company on the said platform would be preserved, in order to, on one hand, respect each company's right to have its data protected, and on the other hand, to avoid creating focal points or exchanges of sensitive information capable of generating tacit collusion. Thus, in principle, the debate did not concern the protection of personal data derived from mass collection of individuals. However, there was a parallel discussion regarding the expansion of the objectives of Competition Law that intersects with the present debate.

49. Indeed, Counselor Gustavo Augusto Freitas de Lima understood that if – theoretically - the joint venture was to establish compliance with environmental goals not provided for in local legislation, and if such goals were to restrict or have the potential to restrict the production of the respective commodities, the joint venture and its executives could be engaged in cartel behavior aimed at reducing production. However, this was just a theoretical inference and Counselor Gustavo voted in favor to approve the joint-venture (DOCSEI 1252016, §16). Councilor Victor Oliveira Fernandes, likewise, acknowledged the role of Competition Defense Law in promoting sustainable initiatives that do not pose competitive risks, without abandoning a traditional paradigm of the consumer welfare standard.

50. The decision of the Presidency of CADE (DOCSEI 1251494) in this case was that the operation would not generate any competitive problem. However, it was mentioned that, while CADE agrees that climate change, among other topics such as sovereignty, consumer rights, gender equality, labor rights (and even Privacy Protection), represent important issues in our society and that certain measures to protect these rights are necessary, there was a concern that cases like this could be used to expand the jurisdiction of the competition defense authority beyond that provided for in legislation and for which it has technical capacity. It was understood that it is not within CADE's jurisdiction to introduce concepts foreign to the traditional scope of competition law, deviating from an orthodox analysis, in order to weigh and assess them as part of our institutional mission, which is competition defense. Otherwise, CADE would “open a Pandora's box” where all sorts of social and political issues could become subject to antitrust analysis.

51. It was understood that it would be unwise to follow a global trend that anything unresolved by another institution (including Privacy concerns) is therefore the responsibility of competition law and antitrust authorities.

3. Final remarks

52. There are some studies that claim that even privacy-focused search engines, such as StartPage, Qwant, and DuckDuckGo fail to protect users’ privacy when clicking ads. (CHOUAKI et al., 2023[22]). On the other hand, if the consumers really value their privacy, they can make use of different VPN softwares, as well as join the movement to "track the trackers" through applications like Privacy Badger[5], Disconnect[6], Ghostery[7], among others. (BOUHNIK and CARMI, 2018[23]; 2016[24]).

[5] https://privacybadger.org/

[6] https://disconnect.me/

[7] https://www.ghostery.com/

53. According to *PricewaterhouseCoopers* [8] eighty-eight percent of global companies say that Privacy Law compliance alone costs their organization more than US$1 million annually, while 40% spend more than US$10 million annually. Furthermore, there are many doubts regarding the best way to implement the protection of personal data protection norms, which can generate legal uncertainty.

54. Niam Yaraghi (2018[25]) refers that some Privacy Law could increase the cost of the services that consumers are so used to receiving free of charge, as consumers will not be able to pay with their information anymore. Also, artificial intelligence inventions are smarter due to the amount of data they collect and analyze. If they do not access much data, one consequence could be lower quality of services and products. So, Regulatory Agencies need to find a proper balance between all these aspects.

55. Bringing the discussion on privacy into the antitrust arena will render the necessary dialogue on various implementable alternatives (that cost differently) in an opaque field, akin to a fragmented, difficult social dialogue with fewer political options. The assessment of a merger is a legally bound activity, where great amount of predictability is desirable.

56. This does not mean that it is not possible to apply competition advocacy tools and cooperate with other entities to address the issue of data protection. Regarding collaboration, CADE endeavors to synchronize its efforts with public policies formulated by other entities, such as the Brazilian National Authority for Data Protection (ANPD) and the Brazilian Secretariat for Consumer Protection (Senacon). This effort occurred within the Brazilian Council for Consumer Protection (CNDC), an entity established in 2020 for governmental agencies to deliberate and harmonize collective initiatives concerning public policies, encompassing competition, data protection, and consumer protection.

57. Moreover, CADE has entered into several technical cooperation agreements with governmental entities: (1) ANPD, to synchronize efforts concerning merger reviews and data privacy violations; (2) Senacon, to exchange technical insights and develop educational programs at the intersection of antitrust and consumer protection; (3) the Central Bank of Brazil, to facilitate information sharing and conduct market studies; and (4) the Federal Prosecution Services, to collaborate on merger reviews, antitrust proceedings, and competition advocacy. These institutional partnerships are expected to aid in resolving conflicts with digital platforms, as exemplified by a case involving Whatsapp. In January 2021, WhatsApp announced changes to its privacy policy, allowing the sharing of users' account information with Facebook, a member of the same economic conglomerate. Users were required to accept the updated policy within a specified timeframe, or else they would lose access to the application. However, in May 2021, due to potential competition concerns arising from the privacy policy change and potential breaches of individuals' data privacy, CADE, along with ANPD, Senacon, and the Federal Prosecution Services, jointly issued a recommendation on the matter. This document stipulated that WhatsApp should not restrict access to the application for users who declined the new terms, and that Facebook should refrain from processing data provided by WhatsApp. Following this coordinated action by the relevant authorities, WhatsApp committed to complying with the recommendations regarding its privacy policy.

58. Therefore, while CADE may not directly address these concerns within the framework of merger assessments, there exists the opportunity for collaborative and coordinated efforts with other entities to navigate issues that intersect with CADE´s activity.

[8] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html

59. In Brazil, also, there is debate over the Complementary Bill PLP 234/2023, which establishes the General Data Empowerment Law and provides for the Brazilian Data Monetization Ecosystem. The project "aims to establish a regulatory framework for data ownership and its monetization." As a justification for the intended regulation, it is considered that technology companies such as Facebook, Google, Amazon, and Microsoft collect vast amounts of personal data from their users, including information about browsing habits, purchasing behaviors, and consumption preferences, and use this data to target ads and deliver personalized content to users. However, users themselves have difficulty monetizing their own data. Thus, in order for the use, sharing, and eventual monetization of data to be carried out by the data subject themselves as a source of revenue, the project proposes some specific rules, inspired by the practices of personal data monetization tools such as DrumWave (FERREIRA, 2023[26]) and dWallet (KING, 2022[27]). So, this proactive path of data empowerment, intelligently leveraging regulation, seems to be more auspicious than the limited and controversial protection that inserting privacy concerns in merger analyses could provide.

References

ADEL, A. (2022), *Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas*, https://doi.org/10.1186/s13677-022-00314-5 (accessed on 14 February 2022). [1]

AU10TIX (2022), *Americans and privacy: new study finds U.S. consumers overwhelmingly concerned about the lack of control over their personal information*, https://www.prnewswire.com/news-releases/americans-and-privacy-new-study-finds-us-consumers-overwhelmingly-concerned-about-the-lack-of-control-over-their-personal-information-301532730.html (accessed on 20 Dezembro 2023). [29]

BAO, J. et al. (2022), *The role of big data-based precision marketing in firm performance*, pp. 246–271. [7]

BHATTACHARYA, S. and ,. BUITEN (2018), *Privacy as a Competition Law Concern: Lessons from Facebook/WhatsApp*, http://dx.doi.org/10.2139/ssrn.3785134 (accessed on 19 Novembro 2023). [17]

BOIT, L. (2022), *Análise acerca da Lei Geral de Proteção de Dados: Direito à Privacidade vs Direito à Informação. Trabalho de Conclusão de Curso.*, Universidade do Sul de Santa Catarina, https://repositorio.animaeducacao.com.br/bitstream/ANIMA/23017/1/TCC%20-%20LEANDRO%20-%20FINALIZADO.pdf (accessed on 19 Novembro 2023). [36]

BOUHNIK, D. and G. CARMI (2018), *Interface Application Comprehensive Analysis of Ghostery*, https://www.researchgate.net/publication/342697991_Interface_Application_Comprehensive_Analysis_of_Ghostery (accessed on 20 Dezembro 2023). [23]

BOUHNIK, D. and G. CARMI (2016), *Functional Analysis of Applications for Data Security and for Surfing Privacy Protection in the Internet*, pp. p. 201-208. [24]

CHOUAKI, S. et al. (2023), *Understanding the Privacy Risks of Popular Search Engine Advertising Systems*, https://inria.hal.science/hal-04228304/document (accessed on 14 February 2023). [22]

CMA (2015), *The Commercial Use of Consumer Data*, https://assets.publishing.service.gov.uk/media/5a7f2a8840f0b6230268dd76/The_commercial_use_of_consumer_data.pdf (accessed on 14 February 2024). [10]

COLL, L. (2015), *Personal data empowerment. Time for a fairer data deal?*, The Citizens Advice Bureau, https://www.citizensadvice.org.uk/Global/Public/Corporate%20content/Publications/Personal%20data%20empowerment%20report.pdf (accessed on 18 Dezembro 2023). [28]

COOPER, J. (2013), *Privacy and Antitrust: Underpants Gnomes, the First Amendment, and Subjectivity*, pp. 1129-1146, https://www.law.gmu.edu/assets/files/publications/working_papers/1339PrivacyandAntitrust.pdf (accessed on 16 August 2023). [18]

CRONIN, B. (1984), *The citation process: the role and significance of citation in Scientific Communication*, Taylor Graham. [20]

DAS, S. and A. KRAMER (2013), *Self-Censorship on Facebook*, pp. 120-127, https://doi.org/10.1609/icwsm.v7i1.14412 (accessed on 19 Outubro 2023). [39]

DATA PRIVACY MANAGER (2023), *20 biggest GDPR fines so far [2023]*, https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/ (accessed on 19 Novembro 2023). [37]

EGGERS, W., R. HAMILL and A. ALI (2013), *Data as the new currency*, https://www2.deloitte.com/content/dam/insights/us/articles/data-as-the-new-currency/DR13_data_as_the_new_currency2.pdf (accessed on 14 February 2024). [6]

FARRELL, J. (2012), *Can privacy be another good?*, pp. 251-265, http://www.jthtl.org/content/articles/V10I2/JTHTLv10i2_Farrell.PDF (accessed on 14 February 2024). [14]

FEIST, G. (1997), "Quantity, quality and depth of Research as influences ons cientific Eminence: is quantity most important?", *Creativity Research Journal*, pp. 325-35. [21]

FERREIRA, S. (2023), *DrumWave apresenta sua carteira digital para monetização de dados: saiba como vai funcionar*, https://epocanegocios.globo.com/tecnologia/noticia/2023/06/drumwave-apresenta-sua-carteira-digital-para-monetizacao-de-dados-saiba-como-vai-funcionar.ghtml (accessed on 20 Dezembro 2023). [26]

FIDELIS, A. (2017), *Data-driven mergers: a call for further integration of dynamics effects into competition analysis*, pp. 189-219, https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/354/175 (accessed on 14 February 2024). [16]

FRANCE, A. and B. GERMANY (2016), *Competition Law and Data*, https://www.autoritedelaconcurrence.fr/en/publications/joint-study-competition-law-and-data (accessed on 16 August 2023). [13]

HOVENKAMP, H. (2023), *Antitrust Interoperability Remedies*, https://scholarship.law.upenn.edu/faculty_scholarship/2814/ (accessed on 14 February 2024). [3]

KING, B. (2022), *Data is money: dWallet da DrumWave chega ao mercado brasileiro em 15/10 para ajudar usuário a monetizar seus dados*, https://fintechsbrasil.com.br/reportagem-exclusiva-fintechs/data-is-money-dwallet-da-drumwave-chega-ao-mercado-brasileiro-em-15-10-para-ajudar-usuario-a-monetizar-seus-dados/ (accessed on 20 Dezembro 2022). [27]

LANDE, R. (2008), *The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern.*, https://ssrn.com/abstract=1121934 (accessed on 15 February). [15]

MAKRIDIS, C. and J. THAYER (2023), *Data Is the New Currency: Antitrust law fails to account for how companies exploit user information to dominate markets.*. [4]

MALIK, L. and A. ABBAS (2024), *Bridging Realms: Artificial Intelligence and the Convergence of Big Data Analytics with IoT.*, https://www.researchgate.net/publication/377805853_Bridging_Realms_Artificial_Intelligence_and_the_Convergence_of_Big_Data_Analytics_with_IoT (accessed on 14 February 2024). [2]

MAYER, J. and J. MITCHELL (2012), *Third-party web tracking: Policy and technology*, pp. 413-427, https://ieeexplore.ieee.org/document/6234427 (accessed on 20 Dezembro 2023). [30]

NUNES, B. and D. GONÇALVES (2017), *Three Ways the Internet of Things Is Shaping Consumer Behavior*, https://www.behavioraleconomics.com/three-ways-the-internet-of-things-is-shaping-consumer-behavior/ (accessed on 14 February 2024). [9]

NUNWICK, A. (2023), *Data to become new currency in the age of AI, says analyst*, https://www.verdict.co.uk/data-to-become-new-currency-in-the-age-of-ai-says-analyst/?cf-view (accessed on 14 February 2024). [5]

OHLHAUSEN, M. and A. OKULIAR (2015), *Competition, Consumer Protection, and the Right [Approach] to Privacy*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2561563 (accessed on 5 September 2023). [19]

POIKOLA, A. et al. (2020), *MyData – an introduction to human-centric use of personal data*, https://mydata.org/wp-content/uploads/2022/07/mydata-white-paper-english-2020-2.pdf (accessed on 20 Dezembro 2023). [33]

REINO UNIDO (2011), *The midata vision of consumer empowerment*, https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment (accessed on 20 Dezembro 2023). [32]

REUTERS (2023), *Amazon pagará US$ 30 milhões por violação de privacidade com Alexa e Ring*, https://g1.globo.com/tecnologia/noticia/2023/05/31/amazon-pagara-us-30-mi-por-violacao-de-privacidade-com-alexa-e-ring.ghtml (accessed on 12 Novembro 2023). [35]

REYNOLDS, P. (n.d.), *The Convergence of Artificial Intelligence and Industrial IoT*, https://www.arcweb.com/industry-best-practices/convergence-artificial-intelligence-industrial-iot (accessed on 14 February 2024). [38]

RISTANIEMI, M. and T. PUUTIO (2016), *The Power of Data: Is It Worth All The Hype?*, https://competitionlawblog.kluwercompetitionlaw.com/2016/07/21/the-power-of-data-is-it-worth-all-the-hype/ (accessed on 14 February 2024). [11]

SARLET, G. and D. RODRIGUES (2022), *A Autoridade Nacional de Proteção de Dados (ANPD) e os desafios tecnológicos: alternativas para uma estruturação responsiva na era digital*, pp. 217-253, https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/issue/view/46 (accessed on 12 Novembro 2023). [34]

SWALLOW, Y. and V. HAKSAR (2019), *The Economics and Implications of Data: An Integrated Perspective*, https://doi.org/10.5089/9781513511436.087.A001 (accessed on 14 February 2024). [12]

TUROW, J. et al. (2009), *Americans reject tailored advertising and three activities that enable it*, http://dx.doi.org/10.2139/ssrn.1478214 (accessed on 20 Dezembro 2023). [31]

YARAGHI, N. (2018), *A case against the General Data Protection Regulation*, https://www.brookings.edu/articles/a-case-against-the-general-data-protection-regulation/ (accessed on 11 Fevereiro 2024). [25]

ZHANG, M. (2023), *Consumer behavior analysis based on Internet of Things platform and the development of precision marketing strategy for fresh food e-commerce.*, https://doi.org/10.7717/peerj-cs.1531 (accessed on 14 Fevereiro 2024). [8]