DATA PRIVACY BRASIL RESEARCH ASSOCIATION'S CONTRIBUTION TO INFORMATION & DEMOCRACY GLOBAL CALL FOR THE WORKING GROUP ON PLURALISM OF NEWS AND INFORMATION IN CURATION AND INDEXATION ALGORITHMS

DataPrivacyBR
Research

The Data Privacy Brasil Research Association is a non-profit civil-society organization that advocates for data protection and other fundamental rights in the context of the emergence of new technologies, social inequalities, and power asymmetries. The association's multidisciplinary team, drawn from various Brazilian regions is developing public-interest research, technical notes, texts analyzing emerging issues, workshops with decision-making agents, and society in general. The Association believes that data protection is one of the foundations of democracy and that it should be seen from the perspective of social justice and power asymmetries. It, therefore, works to promote a data protection culture and ensure that digital rights are fundamental rights for everyone, conducting publicly available surveys, guided by a strong social commitment and with ethical funding. For more details about the organization, the impact of its projects, and how its research is supported, visit **www.dataprivacybr.org**.

Press

For further explanations about the document or for interviews, contact the Association at **imprensa@dataprivacybr.org**

This revisioned contribution is part of the project Amplifying Global South Voices in Digital Rights Policymaking, funded by National Endowment for Democracy (NED).

Authors

Bruno Bioni and Mikael Servilha

Directors

Bruno Bioni and Rafael Zanatta

Project coordinators

Mariana Rielli and Marina Meira

Project leader

Johanna Monagreda

Researchers

Eduardo Mendonça, Gabriela Vergili, Hana Mesquita, Helena Secaf, Jaqueline Pigatto, Júlia Mendonça, Marina Garrote, Mikael Servilha, Nathan Paschoalini, Pedro Saliba e Thaís Aguiar

Advocacy Analyst

Vinícius Silva

Administrative and Communication

Elisa Bayón, Erika Jardim, Horrara Moreira, Júlio Araújo, Layanne Gayofato, Rafael Guimarães, Roberto Junior, João Paulo Vicente, Matheus Arcanjo e Willian Oliveira

How to cite this document

BIONI, Bruno; SERVILHA, Mikael. Data Privacy Brasil Research Association's contribution to Information & Democracy Global Call for the Working Group on Pluralism of News and Information in Curation and Indexation Algorithms. Associação Data Privacy Brasil de Pesquisa, 2022.

Introduction

Last October, team members Bruno Bioni and Mikael Servilha submitted a contribution on Data Privacy Brasil Research Association's behalf to the **Global Call of the Information & Democracy Forum**. The call came from the Working Group on Pluralism of News and Information in Curation and Indexation Algorithms, which was developing its recommendations on mitigating and remedying the harms caused by curation and indexation algorithms. In this format, Data Privacy Brasil's contributions focused its efforts on privacy and data protection aspects.

We contributed to six questions proposed by the working group. All of them, which were situated precisely within the scope of privacy and data protection, was based on the following general proposition: "If we were to create a regulatory framework to minimize the impacts of profiling and techniques (such as recommendation systems and personalized content curation processes) on individuals' privacy". This initial provoking proposition favored the construction of an interesting line of argumentation built on the answers to the proposed questions.

It is expected that this contribution does not find an end in itself but that it stimulates deeper debates on the questions addressed.

QUESTION 1

Would this be necessary, or can users rely on existing privacy or data protection laws and regulations to control how their personal information is used?

In Data Privacy Brasil evaluation, in most cases, existing privacy and/or data protection regulations do not necessarily ensure sufficient protection to minimize the impacts of profiling on individuals' privacy. A brief empirical review of Brazil can provide good insights into this matter, both to: (i) validate this tendency of privacy and data protection laws be and regulations to be insufficient in various realities to minimize the impacts of profiling; (ii) provide the experience of some important Brazilian-related laws that, preserving due proportions, serve as additional barriers to contain and question abusive profiling practices. In synthesis, such instruments can encompass more closely/objectively these topics, which an existing privacy/ data protection law may not cover completely.

In addition to the *Lei Geral de Proteção de Dados*[1] (LGPD), the Brazilian Comprehensive Data Protection Law, Brazil has the *Código de Defesa do Consumidor*[2] (Consumer Defense Code) and the *Marco Civil da Internet*[3] (Civil Rights-Based Framework for Internet) as relevant laws regarding the protection of personal data. **Despite the fact that essential advances were conquered since such laws were passed, promoting transparency duties and a broader logic of informational due process (e.g., right of explanation and review of automated decisions), they are still insufficient**. These laws still do not capture all the more systemic side effects from a more diffuse perspective for a **healthier informational ecosystem**. This again reinforces the need to create a robust regulatory framework to minimize the impacts of profiling and techniques on individuals' privacy.

Given this picture, we assess that the Brazilian legal-regulatory infrastructure could be improved from three main axes: artificial intelligence (AI); fake news, disinformation, and freedom on the Internet; and competition.

---

1 See the LGPD, Law 13.709/2018, available (in Portuguese) at: **http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm**.

2 See the Código de Defesa do Consumidor, Law 8078/1990, available (in Portuguese) at: **http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm**.

3 See the Marco Civil da Internet, Law 12.965/2014, available (in Portuguese) at: **http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm**.

The Law 12.529/2011 that structures the Brazilian System for the Defense of Competition[4] (SBDC, initials in Portuguese) is dated 2011. The SBDC is formed by the Administrative Council for Economic Defense (CADE, acronym in Portuguese) and the Secretariat for Economic Monitoring of the Ministry of Finance. The Brazilian government defines CADE's mission as the commitment to ensure free competition in the market, being the entity responsible, within the scope of the Executive Branch, not only for investigating and deciding on competition matters but also for promoting and disseminating a culture of free competition.

Last year, the Data Privacy Brazil Research Association collaborated and published a discussion paper on data-centric acquisitions, which focused on episodes and cases of acquisitions involving US technology companies. For this research, led by Lucas Griebeler da Motta, the overall purpose was to emphasize the importance of capturing data-centric acquisitions in digital markets[5]. As a specific goal, the paper focused on contextualizing some recent debates related to acquisitions in the digital sphere and on demonstrating that the current notification criteria provided for in Law 12. 529/2011 are insufficient to capture potentially monopolistic transactions in technology markets.

In this sense, we agree that with specific adjustments to the competition law and how CADE acts, we can move towards a progressive expansion of rights, gradually moving towards a more contestable and fair digital market. This, however, should be without losses to more abrupt legislative movements, as the European Union did with the Digital Services Act (DSA) and the Digital Market Act (DMA).

The main issues identified in Griebeler´s work refer to the inadequate criteria for **notification of mergers and to procedural rules that lead to improvements**. Among these, the paper responds to this problem by suggesting the creation of a multisectoral system in which everyone can register to receive information about the notification of concentration automatically acts in certain sectors, in particular, with the National Authority for the Protection of Data (ANPD) always "notified for each operation potentially involving the acquisition and/or possibility of consolidating databases with users' personal information".

4 See the Brazilian Competition Law, 12.529/2011, available (in Portuguese) at: **http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/Lei/L12529.htm**.

5 MOTTA, Lucas Griebeler da. A MULTIJURISDICTIONAL ANALYSIS OF DATA-DRIVEN MERGERS: CURRENT ASSESSMENT AND PUBLIC POLICY PROPOSALS FOR BRAZIL. São Paulo: Data Privacy Brasil Research Association, 2021. Available at: **https://www.dataprivacybr.org/wp-content/uploads/2021/11/dpbr_data_driven_mergers_english.pdf**.

Regarding fake news, disinformation, and freedom on the Internet, in Brazil, the draft bill on fake news (PL 2630)[6], which has been addressing these aspects, is under legislative debate. More specifically, this bill brings rules regarding profiling in the electoral context. About this bill, in 2021, the Data Privacy Brasil Research Association prepared a technical note, offering a reading of the issue from a technical data protection perspective[7]. Our contribution pointed out, especially for members of Congress, why the bill 2630/2020, in its format at the Chamber of Deputies, collides with the rights to privacy, protection of personal data, and other fundamental rights[8]. Such analysis was primarily legal, focusing on some of the provisions' (un) constitutionality.

In this technical note, we propose two specific articles to be included in the draft of the Fake News bill, aiming to cover the issue of profiling in electoral propaganda:

Suggested article I:

> The social media providers that provide promotion of electoral propaganda or content that mention a candidate, coalition or party must make the entire ad set available to the public for checking purposes by the Electoral Court and other purposes, including:
>
> > VI - the techniques and categories of profiling
> > VII - electronic copy of the messages and the name of the responsible for authorizing your shipment.
> > VIII- the links to the registration if the electoral announcements are displayed

---

6 See PL das Fake News, bill 2630, available (in Portuguese) at: **https://www25.senado.leg.br/web/atividade/materias/-/materia/141944**.

7 See AGUIAR, Thaís; BIONI, Bruno; FAVARO, Iasmine; KITAYAMA, Marina; RIELLI, Mariana; VERGILI, Gabriela; ZANATTA, Rafael. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020. São Paulo: Data Privacy Brasil, 2021. Edição revisada e ampliada por AGUIAR, Thaís; BIONI, Bruno; MESQUITA, Hana; PIGATTO, Jaqueline; VERGILI, Gabriela. Available (in Portuguese) at: **https://www.dataprivacybr.org/wp-content/uploads/2022/04/dpbr_ong_nota-tecnica_plfakenews.pdf**.

8 It is worth noting that, at the time of this technical note, we opposed a traceability provision present in the draft of the bill we analyzed. The proposal in question advocated for tracking the messages shared with more than five users to identify the user who originally shared the message. This would occur from the extension of the data retention regime by message application providers. Thus, the project determines that information (who forwarded it, date and time of forwarding, and the number of users who received it) from messages that, within fifteen days, have been sent to at least five people to trace the path taken by the message. So reaching its origin. Thus, this assumes that such tracking was technically and legally possible. However, there is no evidence, study, or case in any part of the world in which the method is effective in combating disinformation. Furthermore, in our technical note, we argue that this provision can violate the constitutional principle of the presumption of innocence and other rights, such as the right to protection of personal data and privacy. We defend, in this sense, a more proportional alternative that makes due criminal prosecution compatible with constitutional rights and principles.

Suggested article II:

> Social media providers must provide mechanisms to provide users with information on the history of content promoted and advertisers that the account has had contact with in the last 6 (six) months, especially:
>
> > I - If any type of profiling technique was applied;
> > II - the profiling categories in which the user was included;
> > III - clear and adequate information regarding the criteria and the procedures used for tillering, in terms of article 20§ 1° of the LGPD.

In the motivation of our suggestions mentioned above, we argue that the profiling techniques have been used in a non-transparent way, creating an informational asymmetry that is too much of the applications and advertisers in relation to the users. For this reason, we defend that it is essential that, whenever there is the practice of profiling, the user can:

1. Know what contents were directed to him from the use of such techniques.
2. Access the categories used by the application and selected by the advertiser to target content.
3. Access clear information about how specific categories have been applied to you.

Therefore, the objective is to ensure that the data subject has equivalent knowledge about the treatment of their information in relation to the agents who use their data. Transparency is one of the principles of our General Data Protection Law. In this case, it allows the user to make a critical analysis regarding the treatment of their personal data and exercise their informational control.

Such a condition, in which a bill related to the data protection law, in the end, goes against fundamental rights (even data protection rights), **demonstrates that the path of construction of a robust regulatory structure, by itself, does not necessarily result in an expansion of rights**. On the contrary, each new step is unique and, in addition to being encouraged and democratically assured, its process must be constantly monitored and discussed so that it moves in the best direction and does not imply a setback. In the case discussed here, the fake news bill has not yet been approved, and Data Privacy Brasil Research Association expects that more debates will be built around the proposal.

On AI regulation, there are currently bills under discussion in Brazil. These first proposals were presented with a language and approach that was very weak and little specialized. Under this, there was a civil society counter-movement, of which the Data Privacy Brasil Research Association was a part. This mobilization provided a necessary course correction. In practical terms, therefore, it led to the creation of a commission of jurists with great experience in the field of technology, with one of the directors of Data Privacy Brazil representing the NGO on the commission.

The expectation today is for a more positive horizon in which one can seek to raise this regulation linked to important tools, such as **algorithmic impact assessment and others of governance tolls**, that can bring greater public scrutiny not only on profiling practices but also of decision automation in the public and private sector. In this sense, we produced a contribution to PL 21/2020[9], which deals with the regulation of AI in Brazil. Through this technical production, we intend to stimulate the debates in Brazil on the subject. In addition, we recently conducted a virtual event on AI regulation from two perspectives as part of a series of workshops[10]. The first focused on learning from the perspective of other countries in the Global South. For this, we had a keynote by Boye Adegoke, from Paradigme Initiative, at the event. The event jumped to an open debate focused on Brazil in a second moment.

In this context, Brazil finds itself today in a framework of already significant achievements. We defend, however, that the consolidation and expansion of rights should continuously guide our efforts. Besides that, we recognize that Brazil is minimally well equipped and is looking forward to new regulations and a more robust toolbox for the governance of a healthier information ecosystem.

9 See PL 21/2020, available (in Portuguese) at: **https://www.camara.leg.br/propostas-legislativas/2236340**.

10 See the event LGPD em movimento: regulação de IA no Brasil e Sul Global, available at: **https://www.youtube.com/watch?v=raZ-glrTuDGA&list=PLtYSjkk1pbNQnOlHIFXs8Se7RBxQlc817&index=3&t=769s**.

QUESTION 2

Could existing laws and regulations be complemented by other interventions? If so, by what types (self, co- or statutory interventions)?

Many of the laws or bills mentioned here derive from co-regulation strategies insofar as many of them (e.g., LGPD and AI and fake news bills) consider the importance of regulatees themselves in translating broad and general rules of conduct to realities of their respective sectors. That is, they establish more general or generic principles, aiming not to limit the scope of the law due to possible language breaks. Added to this, they dedicate sections to indicate openings for movements exogenous to the law and open for organization and development of good practices.

The best example is the possibility that codes of good conduct are approved or even validated by regulatory bodies and authorities, DPAs - for example. The issue of good practices is even provided for in section II of the LGPD, dedicated precisely to dealing with Good Practices and Governance. Section III of the Fake News PL also approaches the issue.

An example of a code of conduct is the one launched in March 2021 by the National Health Confederation of Brazil. In this document, the conference says:

> "It is, therefore, a true framework of governance and good practices, since the text presents itself as the first Code of Conduct for Service Providers Health for GDPR compliance. The initiative, in addition, to guide as to the conduct to be practiced by hospitals and private laboratories aims to encourage innovation with responsibility and consolidate the trust of the holders of data in the health sector"(Our translation)[11].

The telecommunications sector recently released a code of good practice for data protection under the LGPD umbrella. In the document, several protocols are established and a separate section is dedicated to the issue of self-regulation[12].

---

11 Código de boas práticas: proteção de dados para prestadores privados em saúde. 2021. Available (in Portuguese) at: **http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf**.

12 CÓDIGO DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PARA O SETOR DE TELECOMUNICAÇÕES. 2022. Available (in Portuguese) at: **https://conexis.org.br/wp-content/uploads/2022/08/Co%CC%81digo-de-Boas-Pra%CC%81ticas-de-Protec%CC%A7a%C-C%83o-de-Dados-para-o-Setor-de-Telecomunicac%CC%A7o%CC%83es.pdf**.

Not by chance, much has been said about co-regulation or regulated self-regulation in the Brazilian context. From this imbrication between state, regulator, and regulated actors, a phenomenon has been observed in which both collaboratively end up governing behaviors.

In this scenario, **regulatory sandbox initiatives** have gained strength - something that was even proposed in the IA draft bill - but which has been underway in the financial system for some time with the Central Bank of Brazil, the Superintendence of Private Insurance and the Commission of Securities.

QUESTION 3

Are there specific industry practices that should be banned or further restricted? If so, do you have evidence of the pros and cons of such bans?

Yes. The argument behind this answer can be evidenced by a simple logical relationship or a basic calculation of benefits and externalities. In this sense, just the fact that the harmful effects of several technologies outweigh their benefits is enough to ban or, at least restrict.

As examples, we mention the facial recognition systems for public security reasons, their bias, and its way of reproducing discriminatory practices and base damages. Many of these damages are of extreme violence. More than that, today, many of these systems are ineffective, error-prone, invasive, facilitate abuse, and provide no mechanism for transparency.

Another activity that urgently needs to be evaluated and discussed is data brokers, whose activity is based on processing personal data. In this sense, the article by Zanatta, Secaf and Mendonça (2021)[13] discussed three central aspects of the applicability of the LGPD to data brokers:

1. The problem of legal bases for data processing
2. The duties applicable to data brokers, considering the intersection of the LGPD with the Consumer Defense Code and the Positive Registration Law
3. The problem of excessive data processing by the data broker, especially when it is impossible for the data subject to know or contest inferential data, is built from crossing his personal data in a previous treatment situation.

More must be done to address the illegalities related to this activity.

Furthermore, we can also underline the current constitutional action process on the Citizen Base Registry and use of sensitive Denatran (Brazilian national transit department) data by Abin (Brazilian intelligence), on which one of the directors of Associação Data Privacy Brasil, as

13 ZANATTA, Rafael; SECAF, Helena; MENDONÇA, Julia. A aplicabilidade da Lei Geral de Proteção de Dados Pessoais aos corretores de dados, in: VILLAS BOAS CUEVA, Ricardo; FRAZÃO, Ana. Compliance e Políticas de Proteção de Dados. São Paulo: Thomson Reuters, 2021, p. 957-988. Available (in Portuguese) at: **https://www.dataprivacybr.org/documentos/a-aplicabilidade-da-lei-geral-de-protecao-de-dados-aos-corretores-de-dados/**.

amicus curiae, contributed from the NGO to the Brazilian Supreme Court[14]. On that occasion, it was argued that the action presents a legal problem not about the interoperability "in itself" within the public administration but about the secondary use of data in a scenario of lack of safeguards on these flows, which creates stimuli on what basis of data is shared without due informational process. Data Privacy Brasil defended, at the time, that there is no presentation of purposes of uses. Although information security is mentioned, the deficient presentation of safeguards can potentially represent serious harm to data subjects.

14 Plenário do Supremo Tribunal Federal – Compartilhamento de dados – Rafael Zanatta (Video in Portuguese). Available at: **https://www.youtube.com/watch?v=fBnp2UJ8ozI&t=3s**.

QUESTION 4

How can regulators meet legitimate regulatory goals that may be raised in connection with curation and indexation algorithms without unduly hindering competition or innovation?

It is necessary, first of all, to have adequate enforcement of the existing rules. Therefore, there will be a condition required to conduct a public discussion that, in fact, **reduces the information asymmetry** of the object to be regulated. Today there is no effective rendering of accounts - the principle of accountability - that allows civil society and even regulators to have an adequate picture of what is intended to regulate

An excellent example of this is the lack of systematic and proper preparation of data protection impact reports and, in the future, algorithmic impact reports. Finally, there is resistance to publicizing such documentation.

That said, the advancement / awareness / regulation to establish these documentary elements would be a first step towards achieving the first and most basic objective: to reduce information asymmetry, which is undoubtedly legitimate, necessary and urgent. still knowing that there are already regulatory tools for that.

QUESTION 5

Can policy interventions help users exercise control over their own data?

In the Brazilian context, the biggest challenge is, considering that the ANPD is a new regulatory body with limited resources[15][16], to establish governance in a network with its peers - regulatory bodies - and with civil society. Added to this is the still weak data protection culture in Brazil. Under this, it is essential to consider that Brazil has had a national consumer protection system for over 30 years. **It may allow the ANPD to act at the macro level and the National Consumer Defense System to do the same in retail to empower the consumer-holder of the data with better control over their data. This should generate trust and favor the understanding of data protection since, in everyday consumer relations, the understanding could be facilitated mainly because the consumer's right is more palatable, given its tradition in Brazilian culture.**

In this same sense of verticalization, civil society has an essential role in strategic cases as a watchdog alongside the primary regulator. It happened (and should still happen) in Brazil when **WhatsApp's privacy policy** was updated. In the last update, in 2021, Brazil was the only place in the world where, after tremendous pressure from civil society, data protection, competition, consumer authority, and the federal public prosecutor got together to act in a coordinated way in the case. All these actors joined forces and put pressure on the company, which backed off. In the end, this became a paradigmatic example of a National Policy intervention to help users exercise control over their own data[17].

15 Until very recently, the ANPD (the Brazilian DPA) did not have budgetary autonomy; it was subordinated to the republic's presidency, which was enough to impose on the Brazilian authority the condition of non-autonomy. However, this formal aspect has changed. Now the ANPD has been converted to autarchy.

16 See the report about a workshop we organized on the independence of data protection authorities together with some Global South partners within the framework of the ADAPT Consortium. Available at: **https://adapt.internews.org/2022/04/20/independence-of-data-protection-authorities-lessons-from-the-data-privacy-learning-series/**.

17 See Decifrando a mensagem do caso Whatsapp enviado pelo grupo de autoridades brasileiras, available at: **https://www.dataprivacybr.org/decifrando-a-mensagem-do-caso-whatsapp-enviado-pelo-grupo-de-autoridades-brasileiras/**.

QUESTION 6

How can meaningful transparency requirements be achieved?

Since the process of building the LGPD, our organization has advocated a different regulatory logic for Brazilian standards. In addition to enforcement and legitimate coercive instruments, a law can also encourage desirable behaviors concretely. In other words, we had the idea that a law - and in the case of the LGPD this would be fascinating - should repress lousy behavior and, on the other hand, reward desirable behavior[18]. Based on this, we established that transparency practices could be favored, as well as the self-regulatory character.

That said, an important agenda that still needs to advance is the publicity of impact reports, on which we have acted throughout the entire regulatory process by the ANPD and, more specifically, in implementing digital identity in Brazil[19].

Not limited to that, one of the big problems in the Global South, and particularly in Brazil, are private messaging platforms such as Whatsapp or Telegram. The sharing of disinformation through these spaces goes beyond the issue of content personalization, directing messages directly to profiles already mapped or whose consent has been given to receive them. This goes back to foundational issues that can lead to content personalization, such as data and metadata crossover. Metadata is a kind of envelope of the communication process, as it encompasses various types of data (i.e., data about the user who performs the communication, location, type of message, the network used, time, and duration). Therefore, they provide a high amount of information that, when aggregated and analyzed, can even allow the behavioral profiling of the individual in a very intrusive manner.

Not limited to that, one of the big problems in the Global South, and particularly in Brazil, are private messaging platforms such as Whatsapp or Telegram. The sharing of disinformation through these spaces goes beyond the issue of content personalization, directing messages directly to profiles already mapped or whose consent has been given to receive them. This goes

18 See Memória da LGPD – Observatório PPD – Orlando Silva – Vídeo 153. Available at: **https://www.youtube.com/watch?v=AdA0m-wsLWRY**.

19 ENTRE A VISIBILIDADE E A EXCLUSÃO: UM MAPEAMENTO DOS RISCOS DA IDENTIFICAÇÃO CIVIL NACIONAL E DO USO DE SUA BASE DE DADOS PARA A PLATAFORMA GOV.BR. Available at: **https://www.dataprivacybr.org/documentos/policy-paper-entre-a-visibilidade-e-a-exclusao-um-mapeamento-dos-riscos-da-identificacao-civil-nacional/?idProject=320**.

back to foundational issues that can lead to content personalization, such as data and metadata crossover. Metadata is a kind of envelope of the communication process, as it encompasses various types of data (i.e., data about the user who performs the communication, location, type of message, the network used, time, and duration). Therefore, they provide a high amount of information that, when aggregated and analyzed, can even allow the behavioral profiling of the individual in a very intrusive manner.

In this sense, what can be observed from the Brazilian case is that the effort of legislative action must aim at how citizens' personal data enhance the targeting of political advertisements and disinformation campaigns. **There is a need for transparency policies, not only regarding the financing of political content but also regarding the entire cycle of processing personal data. The exposure of profiling techniques and accountability for the use of personal data is characterized as a key element of this complex phenomenon which is disinformation**. The disinformation problem on Whatsapp can be tackled by investigating "digital marketing" and "digital strategy" business models that rely on illegally obtained personal data. Increasing personal data protection rights and exploring how these markets operate (the way WhatsApp group management services work) is a more cautious and strategic way of tackling the problem.

Putting transparency in a broader context, there is some consensus on the need for greater accountability around ad targeting and data use. That is, how citizens' personal data leverage the targeting of political advertisements. How individuals' personal information is collected and processed for this type of use needs to be evidenced. In the global scenario, this is already understood as the key to the problem of disinformation[20].

Both in the use of algorithms and in the crossing of the data that feeds them, the collection, storage, profiling techniques used and the reasons for certain messages to be directed to specific groups are not practices clarified by controllers or operators, which is a problem immediately related to the absence of a robust data protection culture[21].

Also, as raised in the global discussions, the clarity of data processing has to be generalized over all types of content promotion, not being restricted to those qualified as political propaganda. This proves to be difficult when placed within the scope of platforms whose business model depends on personalizing content through algorithms.

---

20 Panoptykon Foundation, ePaństwo Foundation and SmartNet Research & Solutions. Who (really) targets you? Facebook in Polish election campaigns. Available at: **https://panoptykon.org/political-ads-report**.

21 CODING RIGHTS e TACTICAL TECHNOLOGY COLLECTIVE. Data and elections in Brazil 2018. Report, October 2018. p.49. Available at: **https://www.codingrights.org/wp-content/uploads/2018/11/Report_DataElections_PT_EN.pdf**.