The turning point of transparency: trade-secrecy claims and the restriction of RAIS database[1]

O ponto de inflexão da transparência: alegações de segredo comercial e a restrição da base de dados da RAIS

El punto de inflexión de la transparencia: alegaciones de secreto comercial y la restricción de la base de datos RAIS

José Antonio Gouvêa Galhardo

https://doi.org/10.36428/revistadacgu.v18i33.996

Abstract: Open government data policies seek to promote transparency, innovation, and public accountability, yet their implementation increasingly collides with expanding claims of trade secrecy. Although the literature identifies multiple barriers to data openness, little is known about how trade-secrecy arguments emerge in administrative practice to restrict access to datasets that were previously public, and how early challenges to such arguments expose inconsistencies in their application. This study examines the interpretative shift through which the Brazilian Ministry of Labor and Employment (MTE) began denying access to the historically open Annual Social Information Report (RAIS) database on the grounds of trade secrecy. Adopting a critical hermeneutic approach and an iterative analysis of six Access to Information Requests (AIR) submitted between 2023 and 2025, the article investigates the justifications advanced throughout the successive administrative appeal levels. The findings show that the trade-secrecy rationale was introduced without technical substantiation, foreseeable harm assessment, or consultation with specialized agencies, and that the first challenges to this shift revealed significant internal inconsistencies. These results highlight how secrecy claims reshape transparency practices and raise broader concerns for the stability and credibility of Brazil's open data policy.

Keywords: trade secrecy, open government, privacy, access to information requests, critical hermeneutics

Resumo: As políticas de dados governamentais abertos buscam promover transparência, inovação e *accountability* pública, mas sua implementação tem colidido cada vez mais com alegações de segredo comercial. Embora a literatura identifique múltiplas barreiras à abertura de dados, pouco se sabe sobre como argumentos de segredo comercial emergem na prática administrativa para restringir o acesso a bases anteriormente públicas, e como os primeiros questionamentos a esses argumentos revelam inconsistências em sua aplicação. Este estudo examina a mudança interpretativa pela qual o Ministério do Trabalho e Emprego (MTE) passou a negar acesso à base de dados da Relação Anual de Informações Sociais (RAIS), historicamente aberta, sob a justificativa de segredo comercial. Adotando uma abordagem hermenêutica crítica e uma análise iterativa

1. Artigo submetido em 02/02/2026 e aceito em 06/05/2026.

CC BY

de seis Pedidos de Acesso à Informação apresentados entre 2023 e 2025, o artigo investiga as justificativas apresentadas ao longo das sucessivas instâncias recursais administrativas. Os resultados mostram que a fundamentação baseada em segredo comercial foi introduzida sem demonstração técnica, sem avaliação de dano previsível e sem consulta a órgãos especializados, e que os primeiros questionamentos a essa mudança revelaram inconsistências internas significativas. Esses achados evidenciam como alegações de sigilo remodelam práticas de transparência e levantam preocupações mais amplas sobre a estabilidade e a credibilidade da política de dados abertos no Brasil.

Palavras-chave: segredo comercial, governo aberto, privacidade, pedidos de acesso à informação, hermenêutica crítica

Resumen: Las políticas de datos gubernamentales abiertos buscan promover la transparencia, la innovación y la rendición de cuentas públicas; pero su implementación choca cada vez más con crecientes reivindicaciones de secreto comercial. Aunque la literatura identifica múltiples barreras a la apertura de datos, se sabe poco sobre cómo surgen los argumentos de secreto comercial en la práctica administrativa para restringir el acceso a bases de datos que antes eran públicas, y cómo los primeros cuestionamientos a dichos argumentos revelan inconsistencias en su aplicación. Este estudio examina el cambio interpretativo mediante el cual el Ministerio de Trabajo y Empleo (MTE) de Brasil comenzó a negar el acceso a la base de datos de la Relación Anual de Información Social (RAIS), históricamente abierta bajo la justificación de secreto comercial. Adoptando un enfoque hermenéutico crítico y un análisis iterativo de seis Solicitudes de Acceso a la Información presentadas entre 2023 y 2025, el artículo investiga las justificaciones formuladas a lo largo de los sucesivos niveles de apelación administrativa. Los resultados muestran que la fundamentación basada en secreto comercial fue introducida sin sustento técnico, sin evaluación de daño previsible y sin consulta a organismos especializados, y que los primeros cuestionamientos a este cambio revelaron importantes inconsistencias internas. Estos resultados ponen de relieve cómo las alegaciones de secreto remodelan las prácticas de transparencia y generan preocupaciones más amplias sobre la estabilidad y la credibilidad de la política de datos abiertos en Brasil.

Palabras clave: secreto comercial, gobierno abierto, privacidad, solicitudes de acceso a la información, hermenéutica crítica

1. Introduction

Open Government Data (OGD) policies have become one of the principal instruments for promoting transparency, innovation, and social accountability in the public sector. Nevertheless, their implementation has increasingly coexisted with rising tensions between the principle of openness and expanding regimes of confidentiality—particularly those grounded in privacy and trade-secrecy protections. In a context of accelerated digitalization and accumulation of large volumes of government-held data, these tensions have become more salient, directly affecting legal certainty and the effectiveness of transparency policies.

The literature documents that governments face substantial organizational, technical, legal, and cultural barriers to implementing OGD policies. Structural limitations, fragmented information systems, and resource constraints coexist with concerns about privacy, risks of re-identification, legal uncertainty (e.g. Feeney et al., 2025; Kempeneer et al., 2023; Mabillard et al., 2024; Rudmark et al., 2024; Tejedo-Romero & Araujo, 2025; van Loenen et al., 2016; Zuiderwijk et al., 2012). Scholars also highlight the strategic invocation of trade secrecy claims to restrict access to public information, as well as the tendency of public bodies to adopt expansive interpretations of legal exceptions, thereby reinforcing a culture of opacity and institutional self-protection (Kempeneer et al., 2023; Mabillard et al., 2024; Possamai & Souza, 2020).

Despite these contributions, significant gaps remain. First, little is known about how legal frameworks themselves generate uncertainty and lead public agencies to withhold information out of precaution or fear of liability (Kempeneer et al., 2023). Second, the literature has not examined how the authorities responsible for overseeing data collected from companies apply the foreseeable harm requirement, introduced in the U.S. by the 2016 FOIA Improvement Act and increasingly relevant to debates on trade secrecy (Varadarajan, 2021). Finally, empirical analysis of the internal coherence of govern-

CC BY

mental decisions—and the practical effects of such restrictive interpretations on researchers, citizens, and firms—remain scarce.

This article is the first output of a broader research project examining how trade-secrecy justifications have been mobilized within Brazil's access-to-information regime. In this initial contribution, we address the following research questions: How does the argument of trade secrecy emerge in Brazilian administrative practice as a basis for restricting access to a previously open database, and in what ways do the first challenges to this shift reveal inconsistencies in that interpretation? The core objective is to analyze emergence of this interpretative shift and its internal inconsistencies, using as a case study (Yin, 2018) the Ministry of Labor and Employment (MTE) change in interpretation regarding the disclosure of the Annual Social Information Report (RAIS) database.

The study adopts a critical hermeneutic approach and draws on Access to Information Requests (AIR) submitted by the author between 2023 and 2025. The analysis considers the historical context of the relevant legislation, the trajectory of Brazil's open data policy, and the interactions among public bodies across the four administrative appeal levels established by the Brazilian Access to Information Law (LAI). The findings presented here are partial: they focus on the turning point of transparency at which the trade-secrecy argument was first invoked to restrict access to the RAIS database, and on a second set of requests in which the rationale for this restriction began to reveal internal inconsistencies.

The article contributes original empirical evidence on the practical application of trade secrecy justifications within Brazil's access to information regime and advances a still underexplored debate in the country: the expansive use of trade secrecy as a barrier to public transparency.

The remainder of this paper is structured as follows. The next section presents the literature on privacy and trade-secrecy concerns in OGD and outlines the Brazilian legal framework. We then describe the methodological approach, present the results, and discuss the main findings, concluding with a proposed research agenda.

2. Background

2.1. Open government data and privacy concern

Research consistently demonstrates that governments encounter significant organizational, technical, legal, and cultural barriers when implementing OGD policies. Despite high expectations, public agencies often lack dedicated institutional structures, strategic leadership commitment, automation, and interoperable systems. These limitations are compounded by chronic shortages of financial and human resources (Hossain et al., 2016; Mabillard et al., 2024; Rudmark et al., 2024; Tejedo-Romero & Araujo, 2025; Zuiderwijk et al., 2012). Internal constraints are further exacerbated by misalignments between Access to Information Laws (ATI), data reuse regulations, and competing legal regimes—such as privacy, data protection, and copyright—which generate uncertainty and hesitation regarding the release of high-value datasets (Kempeneer et al., 2023).

A fundamental tension exists between openness objectives and the protection of legitimate rights. ATI frameworks emphasize the citizen's right to information, whereas data protection legislation focuses on mitigating risks associated with the disclosure of sensitive information (Kempeneer et al., 2023). Privacy legislation—most notably the European General Data Protection Regulation (GDPR)—is frequently cited as one of the most significant barriers to OGD (Kulk & van Lan Loenen, 2012; Zuiderwijk et al., 2012). While privacy law requires personal data to be collected for specific and legitimate purposes, open data policies are designed to enable unrestricted reuse. Consequently, once data are classified as personal— including cases in which re-identification is deemed possible— their disclosure as open data becomes unlawful, as governments cannot control subsequent uses (Kulk & van Loenen, 2012; van Loenen et al., 2016).

Advances in artificial intelligence have intensified these concerns. Scholars warn that anonymized datasets can be cross-referenced with other publicly available information, enabling re-identification and creating ethical and legal dilemmas for data controllers (Feeney et al., 2025; Hossain et al., 2016; Rudmark et al., 2024; van Loenen et al., 2016). Data considered non-identifiable today may become identifiable in the future due to new computational techniques or the emergence of additional third-party datasets (Kulk & van Loenen, 2012; van Loenen et al., 2016).

Fears that open data may be exploited by data brokers—such as for population profiling, discriminatory practices, or exposing individuals to "physical or subjective harms" (Borgesius et al., 2015, p. 2090)—further discourage disclosure. Once released openly, data can be replicated indefinitely, li-

CC BY

miting the State's ability to guarantee rights such as access, correction, or erasure. As a result, public bodies often avoid releasing high-value datasets and instead publish only low-risk information, thereby undermining the innovation, accountability, and economic development potential envisioned by OGD policies (Hossain et al., 2016; Zuiderwijk et al., 2012).

2.2. Open government data and trade secrecy

Tensions similar to those observed in the privacy domain also arise in relation to trade secrecy. The disclosure of business data collected through regulatory, or oversight functions may harm competitive dynamics by granting rivals a "free advantage" (Mortent, 2023). Governments may also face reduced cooperation from firms, which may refuse to provide information, conceal it, or demand confidentiality guarantees (Mortent, 2023; Mylly, 2024). In addition, public agencies risk exposure to litigation for damages, and in some jurisdictions public officials may even face criminal liability for disclosing information protected under statutory exceptions to access (Mortent, 2023; Varadarajan, 2021).

At the same time, firms may strategically invoke trade secrecy claims to shield illegal, unethical, or unsafe practices from scrutiny (Mortent, 2023; Stewart & Sanders, 2019). This form of "informational insulation" (Katyal, 2019) enables companies to restrict access not to protect innovation, but to avoid accountability (Mortent, 2023; Mylly, 2024; Stewart & Sanders, 2019). Regulatory capture may further reinforce this dynamic, leading agencies to prioritize corporate secrecy over public interest considerations (Mortent, 2023). In the United States, judicial developments have expanded the scope of Free of Information Act (FOIA) Exemption 4, shifting from a requirement of "substantial competitive harm" to a more permissive standard based on customary confidentiality (Varadarajan, 2021). This expansion has enabled agencies to withhold a broader range of information, undermining oversight in technology-intensive sectors and complicating the disclosure reliable information (Mortent, 2023; Varadarajan, 2021). Excessive secrecy may conceal critical safety risks, as illustrated by the Boeing 737 MAX case, in which lack of transparency hindered the early detection of fatal defects (Mortent, 2023).

In response to these risks, scholars observe a gradual shift away from a "open data for all" paradigm toward alternative disclosure pathways. These include licensing agreements prohibiting re-identification, controlled-access environments ("safe rooms"), and tiered-access models that differentiate between unrestricted, restricted, and confidential data (Borgesius et al., 2015; van Loenen et al., 2016).

Cultural and bureaucratic factors also hinder OGD implementation. Public agencies often fear that disclosure may expose administrative failures, generate litigation, or reduce their control over valuable informational resources (Feeney et al., 2025; Rudmark et al., 2024; Zuiderwijk et al., 2012)—what some authors describe as bureaucratic "survival weapons" (Hossain et al., 2016). These concerns contribute to a form of "tunnel vision," in which civil servants focus excessively on legal compliance and risk avoidance, reinforcing a "culture of opacity" (Feeney et al., 2025 Kempeneer et al., 2023; Mabillard et al., 2024; Possamai & Souza, 2020; Zuiderwijk et al., 2012). Governments may also misuse legal exceptions to deny access (Mabillard et al., 2024). In Brazil, procedural barriers created by decrees and infra-legal norms, as well as claims of disproportionate administrative burden, frequently obstruct access (Possamai & Souza, 2020).

A growing research agenda addresses these tensions between trade secrecy and open data. Scholars highlight the need to examine how organizational culture and data-protection laws shape disclosure practices (Tejedo-Romero & Araujo, 2025), to monitor the persistence of procedural barriers such as claims of "additional work" while assessing whether proactive transparency reduces request burdens (Possamai & Souza, 2020). Another emerging priority concerns the impact of AI-driven de-anonymization on the willingness of public bodies to release sensitive datasets (Feeney et al., 2025).

This research builds on Kempeneer et al. (2023) concern on how legislation aimed at promoting transparency can, paradoxically, create uncertainty and prompt public agencies to withhold information out of unfounded fear of legal consequences. It therefore investigates whether the authorities responsible for overseeing data collected from companies—and, especially, the bodies that adjudicate freedom-of-information appeals—apply the foreseeable harm requirement, as introduced by the 2016 FOIA Improvement Act (Varadarajan, 2021).

2.3. Legal framework evolution in Brazil

Brazil's Access to Information Law (LAI)[2] establishes that publicity is the rule and secrecy the

2. Brazil (2011), Access to Information Law.

CC BY

exception in public administration, restricting confidentiality to information essential to the security of society and the State. Although the justification of secrecy requires demonstrating actual harm, scholars note that the LAI does not explicitly codify a harm-assessment test, unlike U.S. FOIA (Ribeiro & Machado, 2019).

The Office of the Comptroller General (CGU), the federal body responsible for adjudicating third-instance appeals in AIR, has clarified that data-protection restrictions may be relaxed when justified by public interest, by the data subject's consent, or by specific legal authorization.[3] Beyond these cases, the LAI recognizes confidentiality in legally defined situations such as banking, tax, communications, judicial, and industrial secrecy related to economic activities carried out by the State or by affiliated entities (art. 22).

Regulatory developments have expanded these boundaries. Decree nº. 7,724/2012 excluded from the LAI's scope business information obtained through oversight or regulatory activities when disclosure could generate competitive advantages for third parties—an interpretation that goes beyond the statute, as it does not require fitting the information into a legally defined confidentiality category, as required by art. 22.

In the criminal sphere, the offense of violating secrets within public-administration systems requires that the protected information be defined by law.[4] The Industrial Property Law[5] governs unfair competition, protecting confidential business information with economic value and not easily accessible, as well as undisclosed test data submitted for regulatory approval, except when disclosure is necessary to protect the public. Sectorspecific laws, such as pesticides and bio-inputs reinforce these requirements.[6]

The General Data Protection Law (LGPD),[7] in force since 2021, introduced broader safeguards for personal and sensitive data, including racial origin, religious belief, political opinion, health, sexual life, and genetic and biometric data. Decree nº. 10.046/2019 classified personal data into biographical, registration, biometric, and genetic attributes. Biometric and genetic data are sensitive; biographical attributes may or may not be. The LGPD also adopts an expansive notion of identifiability, recognizing that cross-referencing with other datasets—such as the National Registry of Legal Entities (CNPJ)—may enable identification.

Parallel to these protections, Brazil's Internet Bill of Rights[8] mandates the open and structured dissemination of public data across all levels of government. The federal open data policy,[9] later assigned to the CGU,[10] requires that datasets be made open unless access is "expressly" prohibited. Registration databases such as the CNPJ are typically published on the Brazilian Open Data Portal (https://dados.gov.br/home) under the Creative Commons Attribution license, which preserves copyright while allowing commercial use and modifications, provided proper credit is given.

Taken together, these developments illustrate a complex legal environment in which transparency mandates coexist with expanding regimes of confidentiality and data protection. This framework, combined with the literature reviewed above, provides the conceptual foundation for the case study presented in the next section.

3. Method

This study adopts an empirical case study design (Yin, 2018) focused on the RAIS database, administered by the MTE. The primary purpose of RAIS is to enable oversight of labor activity in the country. Until 2022, RAIS data—containing the number of formal employees per CNPJ—were routinely disclosed through AIR. Beginning in 2023, however, the MTE—initially influenced by the LGPD—started denying access on the grounds of trade secrecy, marking a significant interpretative shift.

The analysis is grounded in critical hermeneutics, drawing on AIR submitted between 26 October 2023 and 8 September 2025. Hermeneutics seeks to understand the meaning of texts by situating them within their historical and institutional contexts,

3. Interpretive Statement nº. 12/2023 (Enunciado nº. 12/2023).
4. Brazil (1940), Brazilian Penal CodeBrazil (1940), Brazilian Penal Code, art. 153 §1-A.
5. Brazil (1996), Industrial Property LawBrazil (1996), Industrial Property Law.
6. Brazil (2002), Law nº. 10,603/2002, art. 3 I and II.
7. (Brazil (2018), General Data Protection Law, art. 5 II.
8. Brazil (2014), Brazilian Internet Bill of Rights, art. 24 V and VI.
9. Brazil (2016), Federal Executive Open Data Policy.
10. Brazil (2019) Decree nº. 9,903, of July 8, 2019.

CC BY

acknowledging that interpretation is shaped by the researcher's prior knowledge and experiences (Gadamer, 1975; Myers, 2004). Critical hermeneutics, in particular, rejects both the positivist ideal of neutral interpretation and the postmodern claim that all interpretations are equally valid. Instead, it emphasizes a reflective, reason-guided evaluation of competing explanations.

This approach is especially appropriate given the author's dual role as both researcher and petitioner. Because the iterative submission of AIRs forms part of the empirical material, the risk of confirmation bias is inherent. Rather than attempting to eliminate this influence—a goal incompatible with hermeneutic inquiry—the method requires making it explicit and subjecting it to critical scrutiny. The author's prior expertise in transparency law and familiarity with federal datasets function as "productive prejudices" in the hermeneutic sense: they shape interpretation but must be continuously examined to distinguish insights from distortions. The dialogical process between expectations, official responses, and evolving interpretations mitigates the risk of unexamined bias and strengthens the plausibility of the analysis.

Data collection followed an iterative process in which each response informed the formulation of subsequent requests, creating what (Schmidt, 2024) describes as a "live archive." This article focuses on the first two analytical groups: (1) the initial rupture, when RAIS data ceased to be disclosed; and (2) the challenges to the application of trade secrecy to non-business entities. Table 1 lists the six requests submitted.

TABLE 1 • ACCESS TO INFORMATION REQUESTS OF THE MTE'S RAIS DATABASE, ORGANIZED BY RESEARCH OBJECTIVE GROUP.

GROUP	AIR	RECIPIENT	SUMMARY[a]	DATE
1	19955.077826/2023-19	MTE	RAIS database with CNPJ 2022	26/10/2023
1	19955.047120/2024-03	MTE	Disclosure of RAIS data previously released	20/11/2024
2	19955.009928/2024-84	MTE	RAIS CNPJ 64.725.872/0001-08	09/02/2024
2	19955.049567/2024-17	MTE	RAIS data for non-business entities	13/12/2024
2	19955.049672/2024-48	MTE	RAIS/eSocial employee-count database for notary offices	16/12/2024
2	19955.051378/2025-87	MTE	RAIS data for non-business entities from 2020 to 2024	08/09/2025

Note. MTE = Ministry of Labor and Employment; CGU = Office of the Comptroller General; AGU = Attorney General's Office; MDHC = Ministry of Human Rights and Citizenship.

[a]Full content and main attachments available for consultation at https://buscalai.cgu.gov.br

In the following section, we present the findings regarding the turning point of transparency.

4. Results

4.1. Breaking point of trade secrecy

The empirical analysis began with the first AIR, submitted on 26 October 2023, which sought access to the 2022 RAIS database, referencing a similar request granted the previous year (03005.130443/2022-96). In response, the MTE denied access based on a recommendation issued by its Legal Advisory Office, which raised concerns regarding potential re-identification of natural persons and the need for due diligence in handling establishment-level data. The Ministry further indicated that that the matter was "under technical review to ensure that the sharing of establishment-level data poses no risk to trade secrecy and complies with applicable laws" (Response, 27/11/2023, AIR 19955.077826/2023-19).

The first administrative appeal contested the denial by noting the historical availability of RAIS datasets from previous years. The appeal was rejected, and the response emphasized the primacy of the Legal Advisory Office's guidance in determining the boundaries of disclosure: "[…] as a technical unit, this coordination follows the legal guidelines formally provided regarding the disclosure and confidentiality of business establishment data." (Appeal Response – First Instance, 04/12/2023, AIR 19955.077826/2023-19). This exchange illustrates the centrality of legal-interpretive authority within the administrative process and the deference accorded to advisory opinions in shaping technical decisions.

The second-instance appeal focused on the possibility of re-identification, noting that the request was limited to the number of employees per CNPJ and did not include salary information—an impor-

CC BY

tant distinction from the precedent cited in the Legal Advisory Office's recommendation. The appeal was again denied, without introducing new arguments.

The matter was subsequently submitted to the CGU. The appeal highlighted that the Legal Advisory Office itself had acknowledged that the requests did not involve access to natural-person data and therefore did not fall under the LGPD scope. Nevertheless, the CGU upheld the denial based on Legal Opinion CGU nº. 148/2024 (15/02/2024) (Legal Opinion CGU nº. 148/2024). Notably, the opinion did not address the alleged risk of reidentification. Instead, it reframed the issue by asserting that disclosure could violate trade secrecy, on the grounds that the Ministry in obtains such information through supervisory functions over economic activity and that its release could confer competitive advantages on other economic agents. According to the opinion, disclosure "[…] may reveal the company's operational capacity to the market, suggest how the company is internally organized, weaken it in relation to its competitors, and negatively impact its business. (Legal Opinion nº. 148/2024/CGRAI/DIRAI/SNAI/CGU, 15/02/2024, AIR 19955.077826/2023-19).

This interpretation represents a significant expansion of the scope of industrial secrecy, arising from the State's direct engagement in economic activity, under Article 22 of the LAI. The opinion extends the notion of "linkage with the public administration" to include the State's supervisory activities over economic agents, thereby enabling reliance on Article 5, §2 of Decree nº. 7,724/2012 to exclude from disclosure business-related information obtained through regulatory or supervisory functions. Moreover, the opinion effectively delegates to each administrative body the discretion to determine whether disclosure could generate competitive advantages, without requiring that such restrictions be grounded in a legally established confidentiality exception, as mandated by Article 22 of the LAI. The opinion also affirms the possibility of revising prior administrative understanding of confidentiality, without addressing the implications for data previously disclosed.

These interpretive developments were subsequently examined in the appeal to the Joint Commission for Reassessment of Information (CMRI), the final administrative instance. The appeal questioned the proportionality of the competitiveness-risk assessment and listed several potential public-interest uses of the data, including policy evaluation, social oversight, and new business development. It also challenged the assumption that employee-headcount data could meaningfully reveal competitive strategies, noting that "the number of employees is only one variable among hundreds or thousands of parameters in a production plant," and that factors such as capital investment, technology, and outsourcing practices play a far more significant role in determining competitive positioning (Appeal – CMRI, 18/02/2024, AIR 19955.077826/2023-19).

The CMRI acknowledged the potential benefits of disclosure but concluded that these were outweighed by the potential risks to companies, thereby upholding the interpretation of trade secrecy as applicable to employee-headcount data. At the same time, the CMRI explicitly rejected the application of the LGPD to the case, clarifying that the law applies exclusively to data concerning natural persons and therefore could not justify the denial (CMRI Decision nº. 334/2024/CMRI/CC/PR, 24/10/2024, AIR 19955.077826/2023-19).

Finally, the CMRI endorsed the CGU's interpretation that the Public Administration may revise its own acts ex officio. This understanding was reaffirmed in CMRI Decision no. 293/2025/CMRI/CC/PR, concerning AIR 19955.047120/2024-03, which sought "exactly the same RAIS data from 2018 to 2021 provided to another citizen in response to LAI request 03005130443202296." The request was denied based on Legal Opinion CGU nº. 148/2024, despite the prior disclosure of the same data. The decision did not address the MTE's own acknowledgment that employee-headcount data is not listed by the Administrative Council for Economic Defense (CADE) among the categories of information considered competitively sensitive, such as costs, pricing, or market strategies (Response - First-Instance, 16/12/2024, AIR 19955.047120/2024-03). This omission constitutes the first external inconsistency identified in the evolving administrative interpretation

4.2. Uncovering an inconsistent argument

A second set of requests was prompted by the observation that the CNPJ registry encompasses a wide range of legal entities, many of which do not operate in competitive markets. This raised the question of whether the trade-secrecy rationale invoked by the MTE and subsequently endorsed by the CGU and CMRI could be coherently applied to employee-headcount data for non-business entities.

The first request in this group sought RAIS data, from 2013 to 2023, for a specific CNPJ (64.725.872/0001-08) belonging to the Instituto Luiz

CC BY

Inácio Lula da Silva, a nonprofit association—although this characteristic was not explicitly mentioned in the request. The MTE denied access based on Legal Opinion CGU nº. 148/2024, arguing that disclosure could confer a competitive advantage. On appeal, however, the CGU overturned the denial, concluding that the rationale did not apply to nonprofit entities: disclosure "[…] does not entail […] harm or loss of competitive advantage to the entity, given that it is an association dedicated to the defense of social rights. (Legal Opinion n° 633/2024/CGRAI/DIRAI/SNAI/CGU, 04/06/2024, AIR 19955.009928/2024-84). This decision introduced an important distinction within the administrative interpretation: the applicability of trade secrecy would depend on the nature and purpose of the entity, rather than solely on the characteristics of the data requested.

Six months later, two additional requests were submitted almost simultaneously. One sought RAIS data for all notary offices (AIR 19955.049672/2024-48), while the other requested data for "all entities that do not engage in economic activity yet operate within a competitive business environment" (AIR 19955.049567/2024-17), explicitly designed to test the boundaries of the trade-secrecy argument.

In the case of notary offices, the MTE again denied access based on Legal Opinion CGU nº. 148/2024. In the first-instance appeal, the requester argued that notary offices, as delegated public services, fall within the category of nonprofit entities for which the trade-secrecy rationale lacked legal grounding. The MTE subsequently released the database but excluded establishments with up to five employees, invoking a renewed concern with personal-data identifiability: "[…] establishments with up to 5 registered employees were disregarded, since this number of records could characterize the data as identifiable" (Appeal Response – First Instance, 20/01/2025, AIR 19955.049672/2024-48).

The second-instance appeal challenged both the plausibility of re-identification and the absence of any legal or technical basis for the five-employee threshold. The MTE upheld the denial, acknowledging that "the law does not expressly determine the level of disaggregation at which information may be considered identifiable," and grounding its position in "technical and doctrinal interpretation." The Ministry simultaneously conceded that no public databases exist that would enable cross-referencing capable of identifying individuals, yet maintained that identifiability remained possible "even if there is no availability of open public databases" (Appeal Response – Second Instance, 31/01/2025, AIR 19955.049672/2024-48). This reasoning reveals a tension between the Ministry's stated evidentiary basis and its asserted risk assessment.

The appeal to the CGU highlighted these inconsistencies, as well as the lack of justification for the five-employee threshold—an approach difficult to reconcile with the federal government's open data policy. The CGU granted the request, but on different grounds: it held that notary offices employees are legally classified as public agents, and therefore trade-secrecy rationale did not apply. This reasoning suggests that, had the request concerned a different type of nonprofit entity, the arbitrary threshold might be maintained despite its lack of explicit justification.

A broader implication emerges from the CGU's opinion: the MTE interprets the risk of re-identification as encompassing not only potential linkages with open government datasets, but also with any personal information available on the internet. The Ministry reiterated this understanding in subsequent submissions, citing potential linkages with institutional websites, social networks, professional registries, municipal transparency portals, and professional associations (Legal Opinion nº. 513/2025/CGRAI/DIRAI/SNAI/CGU, 11/02/2025, AIR 19955.049672/2024-48). This expansive conception of identifiability significantly broadens the scope of data considered sensitive and has direct implications for open-data governance.

The request concerning non-business entities (AIR 19955.049567/2024-17) explicitly referenced Legal Opinion nº. 633/2024/CGRAI/DIRAI/SNAI/CGU, which had supported disclosure in the Instituto Lula case. The dataset released by the MTE, however, was incomplete. A revised dataset submitted in response to the appeal contained inconsistencies when compared with the initial release. The MTE declined to consider the second-instance appeal, citing lack of clarity in the request—a position subsequently endorsed by the CGU (Legal Opinion nº. 515/2025/CGRAI/DIRAI/SNAI/CGU, 25/02/2025) and the CMRI (CMRI Decision nº. 336/2025/CMRI/CC/PR, 09/05/2025, AIR 19955.049567/2024-17). This outcome suggests that procedural arguments may serve as a mechanism for limiting scrutiny of inconsistencies in data disclosure.

A similar pattern emerged in the request concerning notary offices. After the CGU overturned the denial, the dataset released by the MTE again contained inconsistencies. In this instance, rather than

CC BY

waiting for review by the CGU or CMRI, a formal submission (19955.036188/2025-30, 06/09/2025) was filed contesting the accuracy of the data. Only after a subsequent complaint (19955.051387/2025-78, 09/08/2025) requesting an investigation into the responsibility of the public officials involved in producing and supervising a response that contained "incorrect, incomplete, or imprecise information",[11] did the MTE acknowledge the inconsistency, attributing it to disruptions caused by the transition from RAIS to eSocial:

> *The reduction in the number of reporting notary offices in 2022 and 2023 does not represent a decrease in the number of notary offices, but rather the effect of the transition between RAIS and eSocial systems, which generated a break in the time series and differences in data coverage. (Response, 12/03/2025, Formal submission 19955.036188/2025-30).10*

These episodes reveal a pattern of interpretive instability and operational inconsistency in the application of trade-secrecy and personal-data-protection rationales. They also highlight the challenges posed by shifting administrative interpretations for the reliability, continuity, and accountability of government-produced datasets. The next section examines these findings in light of the broader breakdown of transparency associated with the expanding use of trade-secrecy claims

5. Discussion

The findings of this study illustrate how personal-data protection concerns—heightened in Brazil by the enactment of the LGPD—have intensified public administration's caution regarding the disclosure of datasets previously released through proactive transparency or in response to Access to Information Requests (AIR). As observed in other jurisdictions, uncertainty about whether information constitutes personal data or may enable re-identification has led agencies to adopt increasingly restrictive interpretations (Kulk & van Loenen, 2012; Mortent, 2023). In the RAIS case, this uncertainty was applied indiscriminately by technical units, without assessing whether the data in question were in fact personal. The expectation that the LGPD would fill the gaps left by the LAI and its regulatory decree (Possamai & Souza, 2020) did not materialize. Instead, the resulting framework diverges significantly from the contextual factors assessment proposed by Borgesius et al. (2015), which requires evaluating the actual risk of harm in light of specific circumstances.

A central pattern emerging from the analysis is the reliance of technical units on legal opinions issued by internal legal advisory offices—typically staffed by AGU attorneys—and on precedents from higher administrative appeal bodies (CGU and CMRI). This mirrors the phenomenon described by Kempeneer et al. (2023), in which public officials rely on judicial or quasi-judicial interpretations as authoritative sources to navigate legal uncertainty. In practice, these opinions and precedents anchor restrictive decisions, even in cases involving non-business entities for which trade-secrecy concerns are conceptually inapplicable. The result is a form of interpretive path dependency that privileges caution over openness.

The initial invocation of personal data protection often operates as a gateway to broader trade-secrecy claims. Once raised, the argument reappears opportunistically to justify restrictions, often under the allegation of potential re-identification. This dynamic aligns with the category of abusive use of exceptions described by Mabillard et al. (2024), in which legal exceptions become tools for obstructing transparency rather than protecting legitimate interests. The risks invoked in the RAIS case were not technically demonstrated and relied on speculative data linkages—not only with open government datasets, but with any dataset available on the internet, including private, closed, or even unlawfully obtained sources. As van Loenen et al. (2016) warn, such an expansive conception of identifiability undermines the feasibility of OGD policies. It is unreasonable to expect technical staff in any public agency to know all existing data sources, even public and lawful ones, or to master all available data-matching technologies to conduct present and future risk assessments of re-identification.

This leads to a critical point: risk assessments concerning personal data protection or trade secrecy were conducted without a clear methodology that considers legislation, interpretive guidance, or consultation with specialized bodies such as the Brazilian National Data Protection Authority (ANPD) or CADE. Given that the foreseeable harm requirement—central to the U.S. FOIA Improvement Act of 2016 (Varadarajan, 2021)—demands a concrete demonstration of how disclosure would cause specific harm, the absence of such consultation is par-

11. The formal submission 19955.036188/2025-30 and the complaint 19955.051387/2025-78 will be available on the author's ResearchGate profile, as these documents are not publicly accessible.

CC BY

ticularly problematic. A proper foreseeable harm analysis would require, at minimum, (i) identifying the protected interest, (ii) demonstrating how disclosure would harm that interest, and (iii) showing that the harm is reasonably foreseeable rather than speculative. None of these steps were observed in the cases analyzed. Instead, agencies relied on generalized assertions of risk, without empirical evidence or sector-specific expertise.

The administration's asserted power to revise its interpretation when new facts allegedly render previously disclosed information confidential introduces an additional layer of uncertainty This raises unresolved questions about the status of data already released, including potential State liability and the legal exposure of individuals who continue to use such data. In the cases examined, the MTE, CGU, and CMRI remained silent on these issues, effectively shifting the burden of uncertainty to the judiciary and to data users.

The partial results of the research presented in this paper indicate that appeal decisions in AIR cases—decisions that could overturn denials of access—tend to privilege business interests over the public interest, exploiting precisely the infralegal grey zone highlighted by Possamai and Souza (2020). This is exemplified by the application of Article 5, §2 of Decree No. 7.724/2012, interpreted expansively to justify withholding information even when the statutory for confidentiality under Article 22 of the LAI is not met. Such interpretations broaden the scope of secrecy beyond what the law prescribes, reinforcing a culture of opacity and institutional self-protection.

An additional issue, still underexplored in the literature, emerges from the cases analyzed. When compelled by higher-level appeal decisions, technical units complied with the disclosure orders, but often reluctantly and in ways that suggest an expectation that requesters would be unable to verify the completeness or accuracy of the information provided. This behavior resonates with (Hossain et al., 2016) notion of "survival weapons," whereby agencies retain control over informational resources to preserve autonomy and avoid scrutiny. The provision of incomplete or inconsistent datasets, whether deliberate or not, poses significant risks to researchers, journalists, activists, and lawyers who rely on government data. In many cases, inaccuracies may stem from operational limitations rather than intentional obstruction, yet they nonetheless constitute a substantive barrier to transparency.

6. Conclusion

This article set out to answer the following research question: How does the argument of trade secrecy emerge in Brazilian administrative practice as a basis for restricting access to a previously open database, and in what ways do the first challenges to this shift reveal inconsistencies in that interpretation? The case of the RAIS database shows that trade secrecy was introduced as a new justification for restricting access to information that had historically been disclosed, and that the first administrative challenges exposed significant inconsistencies in the reasoning adopted across appeal levels. The analysis demonstrates how concerns initially framed as personal-data protection were gradually reframed as trade-secrecy risks, often without technical substantiation, methodological rigor, or consultation with specialized bodies such as the ANPD or CADE. This interpretative shift reflects broader patterns identified in the literature, including the abusive use of exceptions, the absence of foreseeable harm assessments, and the reinforcement of a culture of opacity within public administration.

The study's main contribution lies in providing empirical evidence of how trade-secrecy arguments are mobilized in practice, revealing the fragility of the administrative reasoning used to justify the restriction of previously open data. It also highlights the structural limitations of expecting technical units to conduct meaningful re-identification or competitive-harm assessments when their decisions are anchored in legal opinions and in precedents, which ultimately shape outcomes against the public interest in transparency and in favor of protecting trade secrecy and institutional self-protection.

A key limitation of this research stems from the chosen method. Critical hermeneutics acknowledges that the researcher's prior knowledge, experience, and values shape interpretation. The author's dual role as petitioner and analyst introduces a potential confirmation bias; however, the method explicitly requires making such preconceptions visible and subjecting them to continuous critical reflection. Additionally, given that the study examines a single federal body and a single dataset, its findings cannot be generalized in a statistical sense. Nonetheless, this does not limit the study's capacity for analytical generalization (Yin, 2018). It offers a revelatory case of an underexplored phenomenon and contributes to a broader longitudinal research project.

CC BY

Finally, this initial contribution opens several promising avenues for future research. Promising research questions include:

a) How administrative bodies operationalize—or fail to operationalize—the foreseeable harm test when applying trade-secrecy or personal-data exceptions.

b) How specialized agencies such as the ANPD and CADE could provide technical guidance for decisions involving data protection and competitive sensitivity.

c) How inconsistencies across federal agencies affect legal certainty and the stability of Brazil's open-data policy.

d) What civil and criminal liability implications arise from retroactively restricting datasets that were previously disclosed.

e) Were the responses provided as a result of appeal decisions that overturned the initial denial of access tested and deemed correct by the applicants?

f) How to address civil and criminal liabilities arising from the shift from open to restricted data?

Together, these lines of inquiry can deepen our understanding of how secrecy claims reshape transparency regimes and help clarify the institutional conditions necessary for a coherent and accountable OGD policy.

7. References

Borgesius, F. Z., Gray, J., & Van Eechoud, M. (2015). Open data, privacy, and fair information rinciples: towards a balancing framework. Berkeley Technology Law Journal, 33(3), 2073–2131. https://doi.org/10.15779/Z389S18

Brazil. (1940). Decree-Law no. 2,848, of December 7, 1940 (Brazilian Penal Code). https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm

Brazil. (1996). Law no. 9,279, of May 14, 1996 (Industrial Property Law). https://www.planalto.gov.br/ccivil_03/leis/l9279.htm

Brazil. (2002). Law no. 10,603, of December 17, 2002. https://www.planalto.gov.br/ccivil_03/leis/2002/l10603.htm

Brazil. (2011). Law no. 12,527, of November 18, 2011 (Access to Information Law). https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm

Brazil. (2014). Law no. 12,965, of April 23, 2014 (Brazilian Internet Bill of Rights). https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Brazil. (2016). Decree no. 8,777, of May 11, 2016. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm

Brazil. (2018). Law no. 13,709, of August 14, 2018 (General Data Protection Law). https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Brazil. (2019). Decree no. 9,903, of July 8, 2019. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9903.htm

Feeney, M. K., Fusi, F., & Pezo, I. (2025). Which data should be publicly accessible? Dispatches from public managers. Government Information Quarterly, 42. https://doi.org/10.1016/j.giq.2025.102008

Gadamer, H.-G. (1975). Hermeneutics and Social Science. Cultural Hermeneutics, 2(4), 307–316. https://doi.org/10.1177/019145377500200402

Hossain, M. A., Dwivedi, Y. K., & Rana, N. P. (2016). State-of-the-art in open data research: insights from existing literature and a research agenda. Journal of Organizational Computing and Electronic Commerce, 26(1–2), 14–40. https://doi.org/10.1080/10919392.2015.1124007

Katyal, S. K. (2019). The paradox of source code secrecy. Cornell Law Review, 104(5), 1183. https://scholarship.law.cornell.edu/clr/vol104/iss5/2

Kempeneer, S., Pirannejad, A., & Wolswinkel, J. (2023). Open government data from a legal perspective: an AI-driven systematic literature review. Government Information Quarterly, 40(3). https://doi.org/10.1016/j.giq.2023.101823

Kulk, S., & Van Loenen, B. (2012). Brave new open data world? International Journal of Spatial Data Infrastructures Research, 7, 196–206. https://doi.org/10.2902/1725-0463.2012.07.art10

Mabillard, V., Esposito, G., Cicatiello, L., Gaeta, G. L., & Pasquier, M. (2024). Barriers to freedom of information: insights from an experiment in Belgium. International Journal of Public Administration, 48(8), 519–531. https://doi.org/10.1080/01900692.2024.2378329

CC BY

Mortent, C. J. (2023). Publicizing corporate secrets. University of Pennsylvania Law Review, 171(5), 1319–1404. https://doi.org/10.58112/plr.171-5.2

Myers, M. D. (2004). Hermeneutics in information systems research. In J. Mingers & L. Willcocks (Eds.), Social theory and philosophy for information systems (pp. 103–128). John Wiley & Sons Ltd.

Mylly, U. M. (2024). Trade secrets and the Data Act. IIC International Review of Intellectual Property and Competition Law, 55(3), 368–393. https://doi.org/10.1007/s40319-024-01432-0

Possamai, A. J., & Souza, V. G. de. (2020). Transparência e dados abertos governamentais: possibilidades e desafios a partir da Lei de Acesso à Informação. Administração Pública e Gestão Social, 12(2). https://doi.org/10.21118/apgs.v12i2.5872

Ribeiro, É. B. Q., & Machado, B. A. (2019). Transparência máxima: as restrições ao direito de acesso a informações no Brasil, Chile e México. Revista de Informação Legislativa: RIL, 56(222), 215–234. http://www12.senado.leg.br/ril/edicoes/56/222/ril_v56_n222_p215

Rudmark, D., Lindgren, R., & Schultze, U. (2024). Open data platforms: design principles for embracing outlaw innovators. Journal of Strategic Information Systems, 33(3). https://doi.org/10.1016/j.jsis.2024.101850

Schmidt, J. J. (2024). Live archives: Freedom of information requests as political methodology. Canadian Geographer. https://doi.org/10.1111/cag.12922

Stewart, D. "Chip," & Sanders, A. K. (2019). Secrecy, Inc.: how governments use trade secrets, purported competitive harm and third-party interventions to privatize public records. The Journal of Civic Information, 1(1), 1–29. https://doi.org/10.32473/joci.v1i1.115657

Tejedo-Romero, F., & Araujo, J. F. F. E. (2025). The influence of organizational resources and administrative processes on the quality of Brazilian open data. Information Technology for Development, 31(4), 1336–1373. https://doi.org/10.1080/02681102.2025.2484616

van Loenen, B., Kulk, S., & Ploeger, H. (2016). Data protection legislation: a very hungry caterpillar: the case of mapping data in the European Union. Government Information Quarterly, 33(2), 338–345. https://doi.org/10.1016/j.giq.2016.04.002

Varadarajan, D. (2021). Business secrecy expansion and FOIA. UCLA Law Review, 68(2), 462–517. https://www.uclalawreview.org/wp-content/uploads/secu-repdfs/2021/11/Varadarajan-68-2.pdf

Yin, R. K. (2018). Case study research and applications: design and methods (Sixth edit). SAGE.

Zuiderwijk, A., Janssen, M., Choenni, S., Meijer, R., & Alibaks, R. S. (2012). Socio-technical impediments of open data. Electronic Journal of E-Government, 10, 156–172. https://academic-publishing.org/index.php/ejeg/article/view/571

José Antonio Gouvêa Galhardo
jose.galhardo@cgu.gov.br
ORCID: https://orcid.org/0000-0002-5685-8116
http://lattes.cnpq.br/3153550577095067
Controladoria-Geral da União

Doutorado em Administração pela Universidade de São Paulo (2022). Mestrado em Ciências Contábeis pelo Centro Universitário Álvares Penteado (2008). Graduado em Engenharia Naval pela Universidade Federal do Rio de Janeiro (1989). Auditor Federal de Finanças e Controle da Controladoria-Geral da União. Experiência em Administração com ênfase em Contabilidade, Auditoria, Políticas Públicas, Tecnologias e Sistemas de Informação.

CC BY