Reglab Trust & Safety Index in the Digital Economy

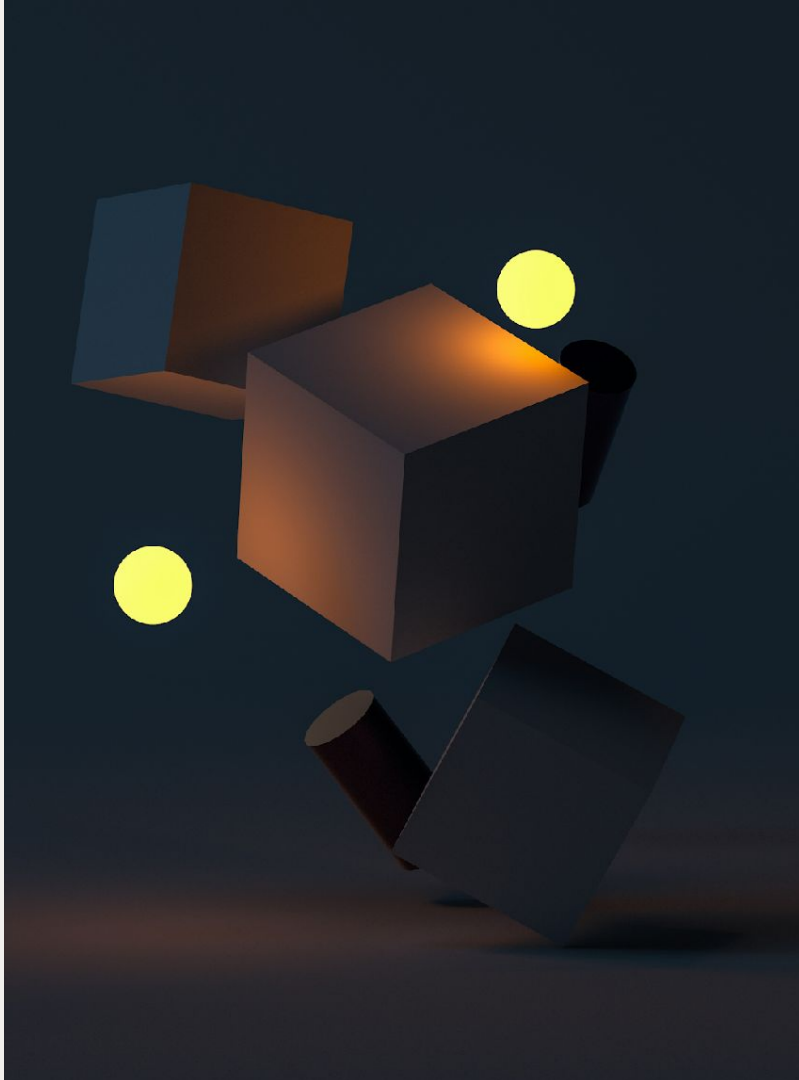
Reglab Trust & Safety Index

Inaugural Report | Q1 2026

reglab
center for strategy & regulation

Data Dashboard

OFFERWISE
Part of the norstat group



About Reglab

Reglab is a private research center that develops studies and strategic consulting for companies, associations, and policymakers operating in technology, media, and regulated markets. We are obsessed with data, rigorous methods, and translating evidence into practical and actionable insights.

Learn more at **www.reglab.com.br**

About the Reglab Index

The **Reglab Trust & Safety Index** (*Índice Reglab de Confiança e Segurança na Economia Digital*) is an applied research initiative designed to systematically measure how Brazilian users perceive trust and safety in the digital environment.

The Index covers different segments of the digital economy, reflecting the **diverse uses and functions of platforms in daily life**. Each category is analyzed independently, respecting its specific characteristics regarding usage, risk, and value perception.

acknowledgements

Executive Director

Pedro Henrique Ramos

Research Director

Marina Garrote

Authors

Pedro Henrique Ramos and
João Ricardo Costa Filho

Researchers

Stephanie Souza, Isabella Crispi and
Izabella Soares

Final Layout

Larissa Camargo

Suggested Citation

RAMOS, P H.; COSTA FILHO, J. R. *Reglab Trust & Safety Index in the Digital Economy*. Inaugural Report – Q1 2026. São Paulo: Reglab, 2026.

About this Report

Inaugural Survey — What does it mean?

This document presents the findings from the first round of the Reglab Trust & Safety Index. Since this is the inaugural edition, the data reported here establishes the indicator's baseline. Consequently, there is no historical data or longitudinal analysis available at this stage. The absolute numbers presented will be normalized in future rounds to establish a benchmark (standard = 1) against which variations will be measured.

- The Index measures user perception rather than the technical performance of the platforms.
- The study relies on a nationwide sample of 1,100 respondents, with a 95% confidence level and a margin of error of ±3 percentage points. Data collection was conducted between March 16 and March 27.
- This material is informational and analytical in nature; therefore, the results should be interpreted with caution, particularly regarding comparative analyses and broader inferences.
- The conclusions reflect the methodological scope available at this time and may be adjusted as subsequent rounds and validations are conducted.

Table of contents

1. Introduction

2. Preliminary Findings

3. Analysis and comments

4. Conclusion and directions

5. Methodology Annex

1. Introduction

Inaugural Report | Q1 2026

1. Why measure digital trust?

The public and regulatory debate surrounding digital platforms has become more intense, politically sensitive, and increasingly influenced by diffuse perceptions of risk, reputation, content, personal data, and user protection.

Fragmentation

Existing metrics are scattered: isolated studies and partial indicators capture only fractions of the problem.

Politicization

Issues such as data protection, disinformation, and safety of minors have shifted from technical debates into the political arena.

The Gap

Brazil lacked a stable, comparable, and replicable instrument capable of measuring perceptions in a structured manner.

1. What is the Reglab Index?

The Reglab Trust & Safety Index is an applied research initiative designed to systematically measure how Brazilian users perceive trust and safety in the digital environment.

Trust

The credibility, reputation, and predictability of a service, including its capacity to maintain user trust even in the face of incidents, controversies, or regulatory pressures.

Safety

Harm prevention, transparency in platform practices, and the perception of protection in daily use. It is about understanding whether the platform is perceived as reliable, secure, and responsible.

1. How the Reglab index works in practice?

1,100	95%	±3p.p.	1
respondents per wave	confidence level	margin of error	initial baseline

Data Collection: National online panel structured by Offerwise, a recognized company in digital research and opinion polls.

Sample: Representative of the connected adult Brazilian population, with quotas based on age group (5 brackets), social class (4 classes), geographic region (5 regions), and gender.

Instrument: 5-point Likert scale ("Strongly agree" to "Strongly disagree"), converted to a 0–100 scale and subsequently normalized to a common baseline. "Don't know" and "Unfamiliar with the platform" responses are excluded from the calculation.

Calculation: Simple arithmetic mean of the 4 dimensions per platform to generate the composite Index. Aggregation by subcategory and category is also conducted via simple average, with no weighting for audience or revenue.

1. The four dimensions of analysis

Each platform is evaluated across 4 dimensions, reflecting overall trust (disposition to trust) and trust in specific attributes (trusting beliefs). The questions were minimally adapted for each category to reflect their specific characteristics.

General Trust
disposition to trust

Global perception of credibility and reliability. Key question: "Generally speaking, I feel I can trust this [Platform]."

Information Integrity
trusting belief

The quality, reliability, and informational security of the content. Key question: "I believe the content and information are reliable."

Data Security
trusting belief

Protection of personal data, privacy, and exposure to digital risks. Key question: "I feel that my personal data and account are secure."

Teenager Protection
trusting belief

Perception of whether the platform is an appropriate environment for minors aged 13 to 17. Key question: "I feel safe allowing a teenager to use this Platform."

MCKNIGHT, D.; CHOUDHURY, V.; & KACMAR, C. *Developing and Validating Trust Measures for e-Commerce: An Integrative Typology*. Information Systems Research. 13, 2002

1. The 5th Indicator: *Trust & Safety*

The **Trust & Safety Indicator** is a composite indicator that synthesizes the perception of Brazilian users regarding trust and safety on digital platforms across the four dimensions. The choice of a synthetic composite indicator follows the methodology recommended by the OECD for multidimensional phenomena. This approach allows for a structured comparison between platforms, categories, and rounds, while simultaneously enabling a granular analysis of each individual dimension.

OECD/JRC. *Handbook on Constructing Composite Indicators: Methodology and User Guide*. OECD Publishing, 2008.

1. What the Index measures

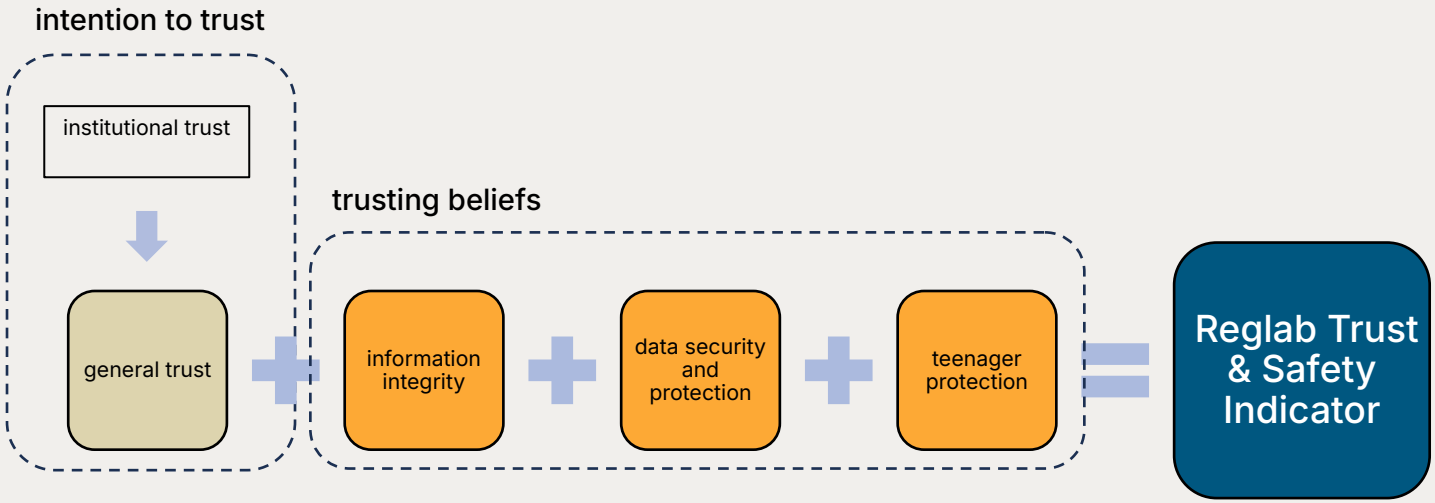
The Index covers different segments of the digital economy, organized into five categories and seven subcategories. Except for the awareness metric, the results are disclosed by category or subcategory.

Category	Subcategory	Evaluated platforms
A. Social Media	—	Instagram, Facebook, LinkedIn, X (Twitter)
B. Streaming	**Catalog VOD**	Netflix, Prime Video, Disney+, HBO Max, Globoplay
	Live & User Generated	YouTube, TikTok, Kwai, Twitch
C. On-Demand Service Platforms	**Transport**	Uber, 99
	Delivery	iFood, Rappi, Zé Delivery
D. AI Chatbots	—	ChatGPT, Gemini, Perplexity
E. Digital Government	—	Gov.br, Meu SUS Digital, Meu INSS

Total: 24 platforms evaluated across 5 categories and 7 subcategories

1. The Reglab Index in brief

Institutional trust refers to the general trust in formal and informal institutions (e.g., "I do not trust the internet") and influences the disposition to trust a platform. It is a difficult aspect to capture in surveys, but it must be methodologically acknowledged (as various inferences are drawn from it) and explored through complementary qualitative methods.



OECD/JRC. *Handbook on Constructing Composite Indicators: Methodology and User Guide*. OECD Publishing, 2008.

1. What is the Index used for?

01

Measure

Systematically measure the perception of Trust & Safety among the Brazilian population regarding digital platforms.

02

Compare

Identify differences in perception across platform categories and demographic profiles.

03

Correlate

Analyze how the perception of trust and safety is associated with industry-specific or national events.

04

Track

Build a time series to observe the evolution of digital trust over time using a replicable methodology.

Methodological Safeguards

The Index was designed to avoid undue comparisons and to ensure analytical consistency.

No Cross-Category Comparisons

The Trust & Safety results are disclosed by category, with no public exposure of individual company scores. Social networks are not compared to delivery services, for example.

Internal Normalization

The results are normalized within each category using their own baseline. Valid comparisons are strictly made within the comparable universe of each service type and over time.

No Audience weighting

Each platform contributes equally to its category's sub-index. The Index measures the perception of trust, not market share.

Exclusion based on lack of familiarity

Respondents who selected "I am unfamiliar with this platform" are excluded from the calculation for that specific platform, ensuring that the results reflect the opinions of those who actually know the service.

1. How will the Index evolve starting in the next edition?

In addition to standardized periodic tracking, the Index will offer new fronts of applied intelligence:

- **On-Demand Surveys** to delve deeper into specific topics using the same respondent base or strategic sub-samples.
- **Expansion of the Monitored Universe**, incorporating new platforms and categories while adhering to strict comparability criteria to prevent distortions.
- **Insights for Qualitative Research**, such as in-depth interviews and focus groups, which can capture nuances that survey methodologies rarely reach.
- **Contextual Impact Analyses**, linking variations in the index to relevant political, social, and media events.
- **Data Dashboard for Partners**, providing expanded access to microdata, filters, and analytical cross-tabulations.

Next edition: July 2026

2. Preliminary Findings

Inaugural Report | Q1 2026

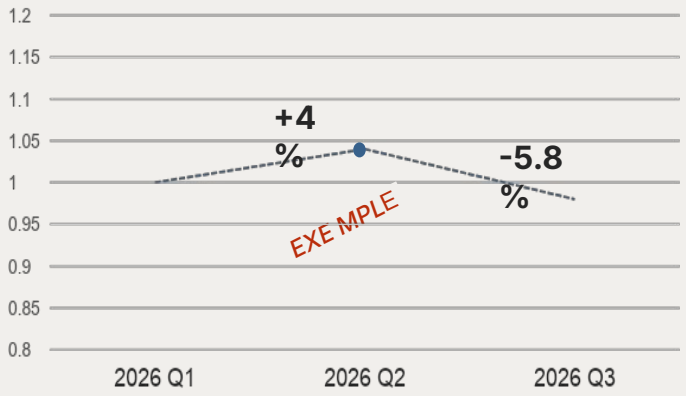
2. What did we measure in the inaugural edition?

This inaugural edition establishes the **Index's baseline of 1**. This baseline serves as the initial reference point for measuring the evolution of trust and safety across future cycles. The objective is to **validate initial data and ensure fair comparability and analytical consistency**, avoiding distortions among platforms of fundamentally different natures.

In this inaugural edition, the data represents a snapshot in time, **highlighting differences across dimensions, service categories, and population segments that caught our attention**, in addition to measuring the level of awareness of the evaluated platforms.

Starting with future editions, **it will be possible to track the evolution of trust over time**, identify gains or losses by category and dimension, and map structural trends and shifts in public perception. This will allow for the validation of initial figures and enable more robust analyses regarding the impact of regulatory decisions, product updates, and relevant events within the digital ecosystem.

example of longitudinal analysis



2. What did we discover in this round?

Even as an initial snapshot, we were able to draw unprecedented inferences regarding the current state of trust and safety perceptions on digital platforms in Brazil. Some of these inferences were drawn from small sample sizes; therefore, their results must be interpreted with caution, as cross-tabulations can render the resulting sub-sample statistically insignificant (see the “direction for future studies” section for further details).

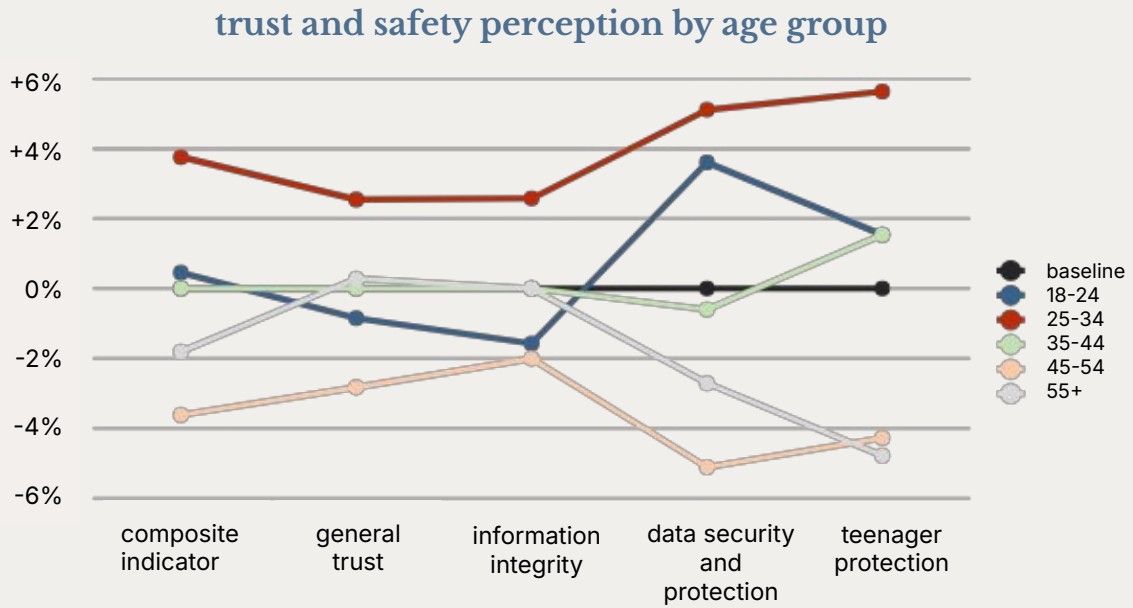
differences across dimensions	Generational gaps and variations between men and women
differences across categories	Gender disparities across categories, regional variations in government apps, and income-based differences in AI chatbots
platform awareness	The majority of the online population has heard of AI applications, yet with significant socioeconomic class disparities

2. The Millennial generation exhibits the highest levels of digital trust, outperforming Gen Z youth across all dimensions

The 25-to-34 age bracket, composed mostly of Millennials, shows higher levels of trust compared to younger cohorts.

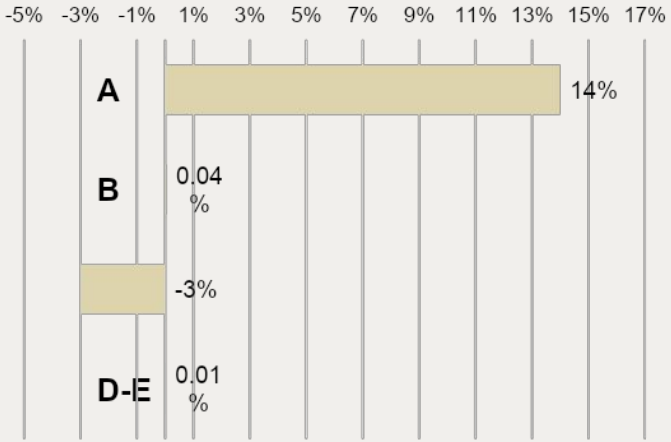
One potential explanation is that this generation experienced the internet of the 2000s as an expansion of possibilities relative to what they had in the 1990s, characterized by greater access to information and open communities.

In contrast, younger individuals grew up with the internet as a given, already dominated by closed communication platforms (e.g., WhatsApp) and visibility highly concentrated around content creators. This environment fosters a retreat from public digital behaviors and a more skeptical, cautious interpretation of the digital space.



2. There is an income-based disparity regarding personal data security and protection

Variation in perception of data security and protection by social class (% over baseline)



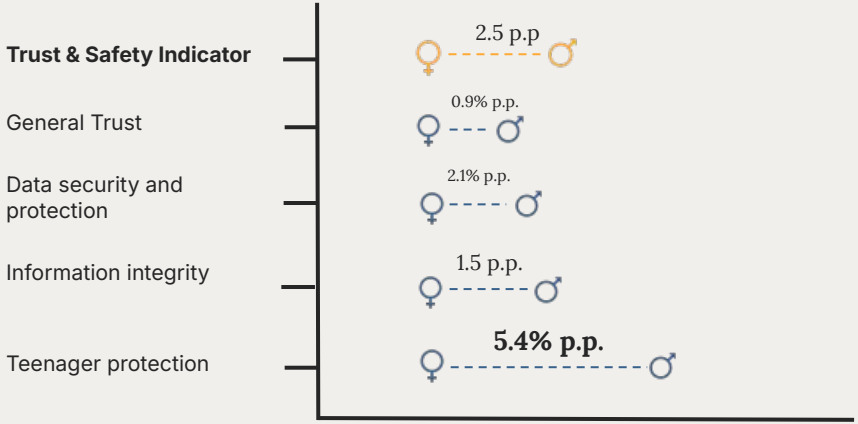
The finding suggests that Social Class A exhibits higher trust because it possesses the material conditions necessary to transform digital security into daily practice rather than keeping it as an abstract concept. When a social group has greater technical repertoire, more formal education, better devices, superior connectivity, and more support to resolve incidents, it perceives a higher degree of control over its digital life.

Conversely, the lower levels of trust observed in Classes C, D, and E may reflect a more concrete understanding of vulnerability and digital literacy inequality, rather than a lack of interest.

Q: "I feel that my personal data and account are secure [on the Platform]." Classification based on the Brazil Criterion (Abep, 2015). Small sample sizes—results must be interpreted with caution.

2. Men and women share similar levels of trust, except when it comes to teenager protection

Gender-Based Differences — Trust vs. Dimensions of Analysis



Men and women evaluate digital trust similarly overall, but their perceptions diverge when the topic involves teenagers.

In Brazil, where caregiving remains heavily gendered and the family holds a central position in social and cultural values, this finding suggests that women tend to demand higher accountability from platforms regarding the prevention of harm to minors.

2. Women also trust ride-hailing apps less than men do

The finding suggests that women incorporate the risk of violence into their evaluation of the service: they tend to trust ride-hailing platforms less because they experience urban mobility under conditions that are structurally more exposed to risk, where safety, incident response, and predictability carry more weight than convenience.

In other words, the disparity in trust does not stem solely from the apps themselves, but from gender inequality within the urban experience.

Perception Differences by Category — Men / Women

categories	p.p.
Social media	**-3.7**
Catalog VOD	-2.3
Live & User Generated Content	**-3.5**
Transport (Ride-hailing apps)	**-5.2**
Delivery	-2
AI Chatbots	-2.3
Digital Government	-0.3

2. Regional differences exist in the perception of information integrity across government apps

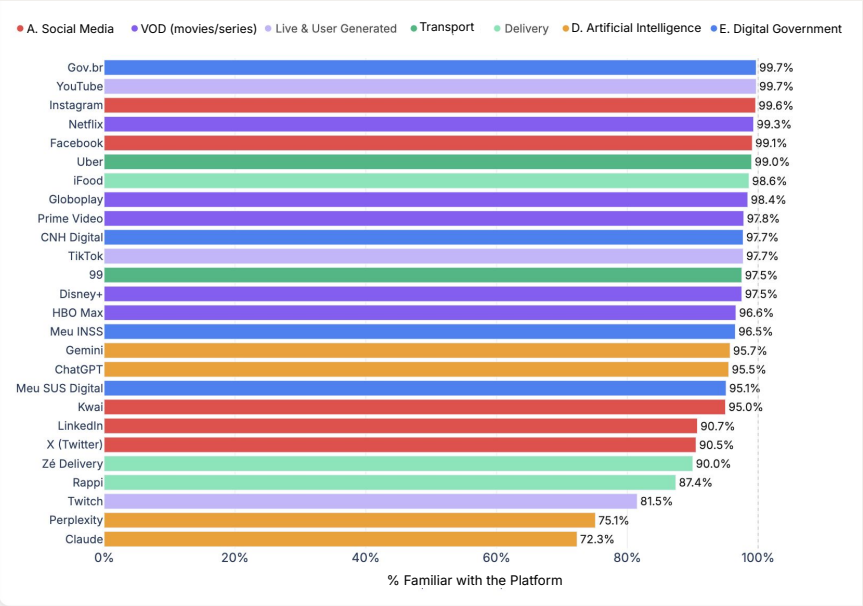
The lower levels of trust in the South and Central-West regarding the content of e-government platforms may reflect, at least in part, lower approval ratings of the federal government in those regions.

Unlike private applications, apps such as Gov.br, Meu INSS, and Meu SUS Digital are not perceived as neutral entities, but rather as visible extensions of public authority. Consequently, the evaluation of the platform may incorporate not only the user experience but also political and institutional trust in the government that operates it.

Q: "I believe that the content and information I find on the public services offered [by these digital government platforms] are trustworthy."

2. Thirteen platforms are recognized by practically the entire online population

- With over 97% of declared recognition, 13 platforms exhibit near-universal awareness among the online population.
- At the top, there are interesting generational breakdowns: YouTube has 100% recognition among the 35-to-44 age group; Facebook and Instagram reach 99.6% among those aged 25 to 34; and TikTok hits 98.7% among the 18-to-24 cohort.
- In the streaming segment, HBO Max shows the largest percentage-point gap between social classes—Classes A/B show roughly 7 p.p. higher awareness than Classes C/D/E.
- Among the less familiar platforms (<90%), Rappi has low recognition in the North and Central-West regions; Twitch sees low penetration among audiences over 45 years old; and Perplexity and Claude exhibit low awareness within Classes C/D/E.



3. Analysis and comments

This section analyzes the research findings, contextualizing them within existing data and specialized literature through the analytical lens of this report's authors.

The inaugural edition of the Reglab Trust & Safety Index in the Digital Economy serves a dual purpose: **to establish a baseline for measuring variations and to demonstrate that digital trust in Brazil is not homogeneous.** Rather, it is an unequal social phenomenon across demographic groups, service types, and dimensions of analysis. Consequently, the index replaces the binary question - "do people trust platforms?" - with more actionable queries for regulation: **who trusts less, in what, in which contexts, and why.**

By treating digital trust as a multidimensional phenomenon, the study's methodology reveals that **digitalization has not reduced social inequality; it has reorganized it**. The income-based disparity in data protection indicates that trust mirrors the unequal distribution of resources. Women's lower levels of trust in transport (Ride-hailing apps), alongside variations regarding teenager protection, show that caregiving roles and structural inequalities in risk exposure deeply impact digital trust. Furthermore, high platform awareness suggests an ecosystem that is mature in reach, yet unequal in adoption.

For public policy, this finding demonstrates that as AI, digital government, social media, and service platforms take center stage, the challenge extends beyond mitigating risks, regulating platforms, or fostering innovation. The core challenge is to **ensure that trust, safety, and the capacity for digital use do not become concentrated solely among groups with greater resources, technical repertoire, and the margin to absorb harm.**

> "digital governance cannot be limited to transparency and platforms' formal duties; it must incorporate real asymmetries and reduce the social vulnerability of users in precarious conditions"

The preliminary findings also reinforce the **risks of concentrating the entire digital agenda within the field of personal data protection**. Translating diverse issues - such as urban violence, information integrity, care for minors, and the legitimacy of the digital State—into a single framework risks oversimplifying the diagnosis and producing narrow responses. While data protection is central, a broader approach is needed—one that recognizes distinct types of risk and harm and adopts varying regulatory instruments, thereby **reinforcing the concept of Trust & Safety as a cross-cutting practice on the digital agenda.**

For policymakers, these initial findings, although preliminary, suggest several pathways forward:

- **Strengthen digital government as an agenda for legitimacy.** It is crucial to design solutions that decouple services like Gov.br from the specific political agenda of incumbent governments, allowing them to be evaluated independently. For instance, the National Digital Government Strategy (*Estratégia Nacional de Governo Digital*) and the Gov.br service points (*Balcão Gov.br*) can advance from merely providing access to offering practical protection, focusing on account recovery, fraud prevention, security literacy, and support for users with lower digital autonomy.
- **Connect teenager protection to the educational agenda.** Programs such as Connected Schools (*Escolas Conectadas*) and Connected Education (*Educação Conectada*) can incorporate digital safety, information integrity, and critical literacy regarding platform use by teenagers, while also extending their impact to parents and legal guardians.
- **Incorporate social inequality into the federal AI policy.** Bills and the Brazilian Artificial Intelligence Plan (*Plano Brasileiro de Inteligência Artificial*) can include metrics for diffusion, adoption, and trust to prevent the advancement of AI from reproducing existing inequalities.
- **Establish continuous monitoring of digital trust.** Periodic metrics on trust and perceived safety can serve as inputs to calibrate ongoing public policies, with a greater focus on vulnerable groups and less reliance on reacting to isolated crises.

4. Conclusion and directions

4. Conclusion

What did we seek to answer with this study?
Rather than starting from isolated cases, industry narratives, or anecdotal impressions, our goal was to build a stable framework to systematically measure how digital trust is distributed across service categories, dimensions of analysis, and social groups. As this is the inaugural edition, its primary purpose was to establish a baseline and demonstrate that digital trust can be treated as a measurable, comparable, and useful variable for more refined regulatory analysis.

And what did we find?
Although these are initial findings, they present a scenario where trust appears less as a mere opinion on "technology" and more as a reflection of social positions in the face of risk. Disparities based on age, income, gender, and region indicate that Brazilians do not evaluate platforms solely based on convenience or familiarity; rather, their assessments stem from experiences of vulnerability, caregiving, and control.

This implies that digital trust is neither uniformly distributed nor entirely dependent on the technical design of platforms. Instead, it is mediated by inequalities in meaningful access, the political climate, the urban experience, caregiving roles, and how each service category integrates into daily life.

Why does it matter?
This matters because the Brazilian regulatory debate still tends to address platforms through overly broad legal categories or isolated crises, whereas the data points to something more complex: digital trust is a socially situated and politically relevant variable. For public policy, this means effective regulations must move beyond the binary opposition between innovation and control. It will be necessary to design responses that account for inequalities in user capacity, concrete protection against harm, institutional legitimacy, and the quality of user experience.

5. Directions for future studies

Below, we outline potential research pathways that can help deepen and validate the research findings presented in this edition of the Index:

- **Generation Z and digital skepticism.** Investigate further, through surveys, in-depth interviews, and longitudinal comparison, why young adults trust less than millennials and whether this correlates with misinformation and the retreat from civic participation.**Gender, caregiving, and risk.** Utilizing correlation and regression analyses with studies on gender-based violence and parental abandonment, examine why women differ more significantly regarding teenager protection and trust transport apps less.
- **Digital government and institutional trust.** Assess, via surveys, whether lower regional trust in public applications stems primarily from user experience or from political perceptions of the incumbent government.
- **AI and the new inequality of adoption.** Examine, through surveys, whether high awareness of chatbots translates into actual usage or if AI is already replicating class inequalities, investigating effective use and digital literacy barriers.
- **Digital trust beyond privacy.** Explore, through focus groups, how users distinguish among data safety, information integrity, teenager protection, and overall trust, thereby validating or challenging existing regulatory frameworks.

reglab

center for strategy
& regulation

methodology annex

Methodology

General information

The Reglab study adheres to rigorous methodological standards to ensure objectivity and transparency. All data and findings are available for independent verification, reinforcing the credibility of our research.

Data collection and analysis took place between March 16 and April 13, 2026, utilizing dual-validation procedures to mitigate bias, alongside specialized software for result organization.

1. Data Collection
2. Data Analysis
3. Bias reduction procedures
4. Other Methodological Limitations
5. Ethical Guidelines
6. Software use

methodology annex

Project Title

Reglab Trust & Safety Index in the Digital Economy — Inaugural Edition, Q1 2026

Research Question

How do adult, internet-connected Brazilian users perceive trust and safety across the main digital platforms that are part of their daily lives, considering different service categories and four specific dimensions of analysis?

Methodology Summary

This study adopts a combined quantitative and qualitative approach, aiming to systematically measure how the connected Brazilian population perceives trust and safety on digital platforms. The study did not intend to audit the technical performance of the platforms or to measure the objective occurrence of harm; rather, it sought to gauge user perceptions through a standardized and replicable instrument. The methodological strategy combined a structured national survey, the application of a five-point Likert scale, and the construction of a composite Trust & Safety index. The index was organized into five categories and seven subcategories of platforms, evaluated across four dimensions: overall trust, information integrity, data safety, and teenager protection. Responses were converted to a 0-to-100 scale, normalized to a baseline of 1, and aggregated by platform, subcategory, category, and overall index. This inaugural edition establishes the baseline for the index, without aiming for longitudinal comparison in this initial round.

2. Data collection

The data collection was conducted through a national online panel structured by Offerwise, a firm specializing in digital research and opinion polls, with a 95% confidence level and a margin of error of ±3 percentage points. Quotas were applied based on age group, social class, geographic region, and gender.

Offerwise operates a proprietary panel, which is fully recruited and managed internally. Participation is voluntary, subject to the acceptance of the Terms of Use and Privacy Policy. Respondents receive incentives upon completing each survey, which tends to enhance engagement and response quality.

To ensure that each respondent is a real and unique individual, multiple layers of control were implemented. These included reCAPTCHA during registration and login to prevent automated access, as well as IP validation and geographic consistency checks (GEO IP), resulting in the permanent deactivation of accounts in the event of confirmed inconsistencies.

Responses were recorded using a five-point Likert scale, ranging from "strongly disagree" to "strongly agree," with two additional options for substantive non-responses: "I don't know" and "I am not familiar with this platform." These non-responses were treated as missing data and excluded from the index calculation for that specific platform.

Collection period

March 16 to 27, 2026

Total sample

1,100 respondents

2. Data analysis

The analysis was conducted using descriptive statistics and the construction of a composite indicator. In the first stage, each response on the Likert scale was converted into a numerical value from 1 to 5 and subsequently transformed into a standardized scale from 0 to 100. In the second stage, the arithmetic mean of the scores for each of the four dimensions was calculated for each platform. The platform's composite indicator corresponded to the simple average of these four dimensional means, assigning equal weight to each dimension. In the third stage, the results were aggregated by subcategory and category, also using a simple average, without weighting for audience size, market share, revenue, or user base.

Since this is the inaugural edition, the absolute values observed in this round serve as the initial empirical baseline for the index. Based on these values, each category was assigned its own base point equal to 1, which will serve as a reference for future waves. The objective of this normalization is to preserve the analytical consistency of the index, prevent improper comparisons between categories of inherently different natures, and make the trajectory of gain or loss of trust in each type of service more visible.

In addition to the composite indicator, the analytical framework preserves the individual reading of each dimension, allowing for a breakdown into overall trust, information integrity, data safety, and teenager protection. The index also allows for disaggregations by age group, social class, gender, and region, provided that the limitations resulting from the reduced *N* in specific subsamples are taken into account.

3. Bias reduction procedures

- **Consolidated theoretical and methodological frameworks:** The structure of the index was based on recognized literature concerning trust measurement in digital environments and the construction of composite indicators.
- **Instrument standardization:** All platforms were evaluated based on statements formulated in simple language and similar structures, with minimal adaptations per category, thereby reducing artificial variations in interpretation.
- **Exclusion of substantive non-responses:** "I don't know" and "I am not familiar with this platform" responses were excluded from the calculation for each platform, preventing mean distortion by respondents who lacked sufficient familiarity to provide an opinion.
- **Comparability controls:** The index was designed to avoid improper comparisons between distinct categories, preserve internal normalization per category, and prevent differences in the nature of services from contaminating the analysis.
- **Dual validation in interpretative stages:** A cross-validation process was adopted for the data analysis stages. At least two researchers reviewed the text and the resulting inferences.
- **Methodological transparency:** Analytical decisions have been explicitly stated since this inaugural edition, including conversion formulas, aggregation criteria, the absence of weighting, and caveats regarding interpretive limits, in line with Reglab's replicability standards.

4. Other Methodological Limitations

Perception vs. Behavior

The Index measures what people believe and feel about the platforms, not what actually occurs with their data or experiences. A platform may possess high technical safety standards and still receive a low score—or vice versa.

Equal weighting across dimensions

The four dimensions contribute equally to the Composite Index. Alternative weighting methods could produce different results.

Equal weighting across platforms

All platforms carry the same weight in the calculation of category sub-indices, regardless of the size of their user base.

Exclusion due to lack of familiarity

Less familiar platforms are evaluated by a smaller subset of the sample, which may introduce selection bias.

Periodicity

The results reflect the specific timeframe in which the survey was conducted. Trust in platforms can fluctuate significantly in response to security incidents, regulatory changes, or high-profile events.

5. Ethical guidelines

- **Personal data processing:** The research involved limited processing of personal data, restricted to the stages of collection, organization, and statistical analysis of the sample. Data were processed in an aggregated format by Offerwise and anonymized prior to delivery to Reglab; consequently, it is impossible to identify, directly or indirectly, any individual respondent from the published information. There is no exposure of individualized responses, nor is there any processing aimed at profiling or automated decision-making regarding the participants.
- **Purpose and suitability:** The data were utilized exclusively for research purposes and the construction of the index, in strict compliance with the objectives communicated to the respondents within the context of the online panel.
- **Data minimization and aggregation:** The published results are aggregated by category, subcategory, dimension, and sociodemographic breakdowns. There is no public disclosure of individual scores per respondent or identifiable personal data.
- **Secrecy and confidentiality:** Individualized participant information is not disclosed. The study operates based on a consolidated presentation of data and structured comparisons between groups.
- **Methodological transparency:** The index methodology has been explicitly described to enable verification, replicability, and appropriate interpretation of the results. This commitment aligns with Reglab's methodological standards for public publications.
- **Responsible data use:** The study measures social perceptions regarding digital platforms and does not aim to reinforce discrimination against groups, brands, or users. The interpretation of the results requires caution, particularly regarding broad inferences and comparisons between subgroups.

6. Software use

SOFTWARE	RESEARCH APPLICATION
Suíte MS Office and Google Workspace	Text editing, spreadsheets, and charts
Claude Cowork, Claude Code and Python	Information systematization, data structuring, support for indicator calculations, database organization, and analytical dashboard design
Gemini 3.1 and ChatGPT 5.3	Brainstorming, organization of front matter elements, ABNT style review, image generation for layout design, and compliance with the Reglab Style Guide
Notion	Text editing, data and file organization, and chart editing

reglab

center for strategy
& regulation

www.reglab.com.br

imprensa@reglab.com.br