

IACHR

2026

THEMATIC HEARING:

*ACCOUNTABILITY OF DIGITAL PLATFORMS
AND THEIR IMPACT ON
HUMAN RIGHTS*



EXECUTIVE SUMMARY

On behalf of the Center for the Study of Law, Justice, and Society (DEJUSTICIA), Colombia; RedPaPaz, Colombia; Artigo 19 Brazil and South America, Brazil; CELS, Argentina; Conectas Direitos Humanos, Brazil; Instituto Alana, Brazil; and Tech Justice Law, United States of America, we requested that the Inter-American Commission on Human Rights (IACHR) hold a thematic hearing on “Accountability of Digital Platforms and Their Impact on Human Rights.” Our request was approved, and the hearing took place in Washington, D.C., on August 4, 2026, during the IACHR’s 197th session.

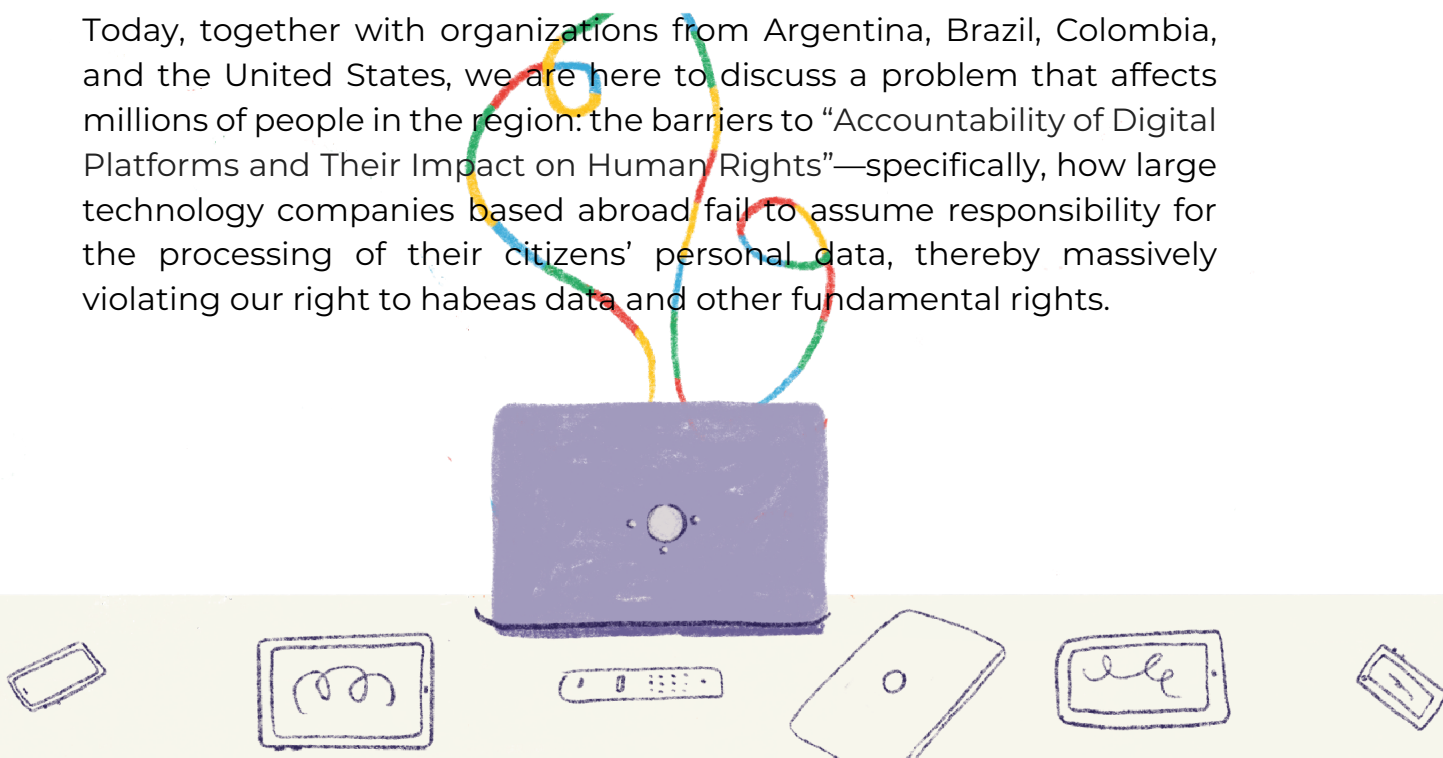
As part of the preparation process for the hearing, the petitioners submitted preliminary briefs to the IACHR, which we have decided to make public due to their academic value. Additionally, as part of the executive summary of this publication, we present the oral statements made by each of the representatives of the petitioning organizations.

OPENING REMARKS: DEJUSTICIA

Honorable members of the Inter-American Commission on Human Rights and rapporteurs, thank you for this valuable opportunity, which reflects the great importance of this issue for the region.

My name is Maryluz Barragán González, and I am the deputy director of the Center for Law, Justice, and Society—Dejusticia. We are a Colombian NGO with more than 20 years of experience defending human rights, democracy, and the rule of law.

Today, together with organizations from Argentina, Brazil, Colombia, and the United States, we are here to discuss a problem that affects millions of people in the region: the barriers to “Accountability of Digital Platforms and Their Impact on Human Rights”—specifically, how large technology companies based abroad fail to assume responsibility for the processing of their citizens’ personal data, thereby massively violating our right to habeas data and other fundamental rights.



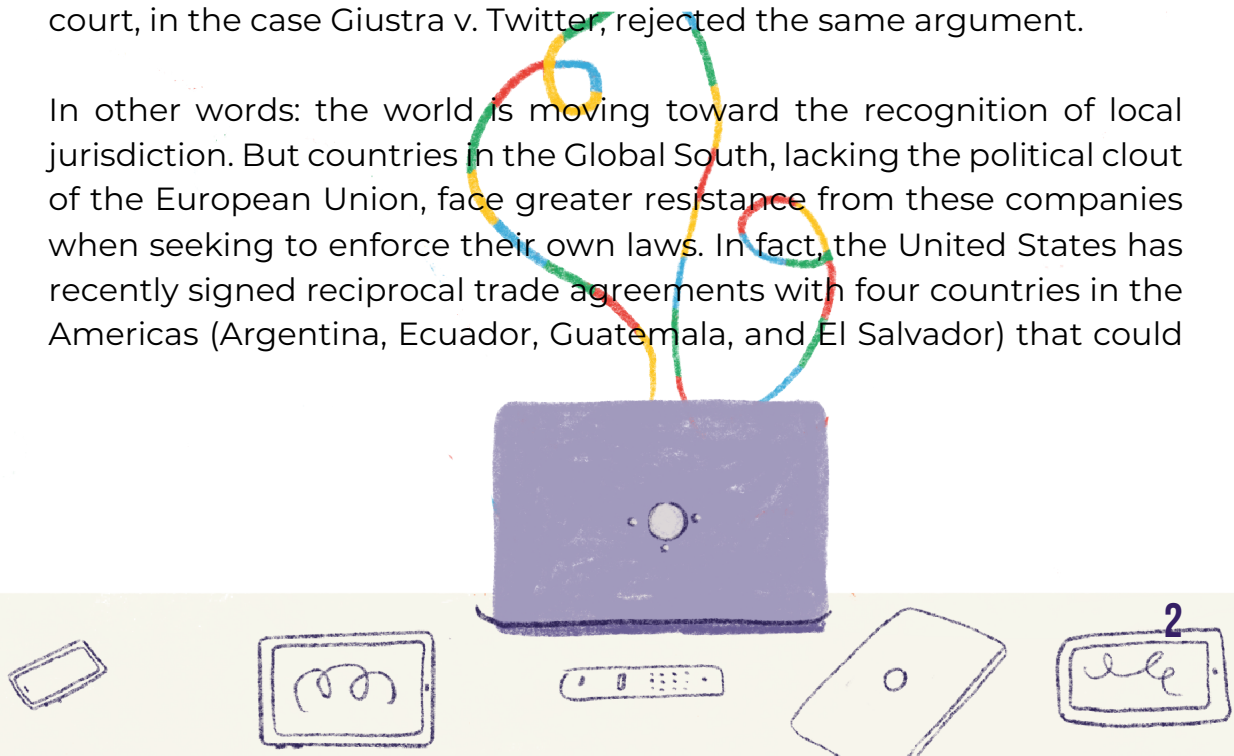
In this first part, I will focus on the issue of jurisdiction and the laws applicable to tech companies. My colleagues will then discuss the specific impacts on issues such as democratic integrity, mental health, and the disproportionate effects on children.

Tech companies base their business model on the massive exploitation of personal data. Through technologies such as cookies, SDKs (software development kits), and pixels (which are installed on users' devices), they collect, store, and monetize intimate information: location, consumption habits, and even health data. Regarding the latter, research from 2022 found that Meta trackers on telehealth websites were sending patients' intimate information to Facebook. All of this occurred within the bounds of the law, which highlights a regulatory gap.

What is important to this Commission is this: that data processing physically occurs in our countries—in the countries of Latin America. The device where the cookie is installed, where the SDK runs, where the pixel is deployed, is in Colombia or any other country in the region. This is not a technicality—it is where the harm occurs.

However, companies like Google have filed lawsuits in Colombia to challenge the jurisdiction of the Superintendency of Industry and Commerce, arguing that the data processing occurs on foreign servers. This position contradicts international and comparative case law trends. The Court of Justice of the European Union, in the cases Google Spain, Google v. CNIL, and Schrems I and II, has been emphatic: companies cannot evade local law by claiming foreign domicile when their activities impact individuals within the territory. Even a Canadian court, in the case Giustra v. Twitter, rejected the same argument.

In other words: the world is moving toward the recognition of local jurisdiction. But countries in the Global South, lacking the political clout of the European Union, face greater resistance from these companies when seeking to enforce their own laws. In fact, the United States has recently signed reciprocal trade agreements with four countries in the Americas (Argentina, Ecuador, Guatemala, and El Salvador) that could



weaken the protection of personal data. My colleague at CELS will explain this in more detail.

This is not an abstract debate. When these companies evade jurisdiction, they leave millions of people defenseless against the manipulative use of their data. We are talking here about concrete impacts on mental health due to addictive designs, risks to vulnerable groups, and undue influence on democratic processes, as we will see in the upcoming presentations.

Therefore, we respectfully request that the Commission consider: First, the preparation of a thematic report or regional guidelines on the responsibility of technology companies regarding human rights—including habeas data—in the region. Second, that it urge member states to strengthen their data protection regulatory frameworks with clear criteria for jurisdiction, in line with existing standards in comparative law.

The fundamental question is simple: Can the world's most powerful companies decide which laws they are subject to? Our position is that they cannot. The protection of human rights cannot depend on the location of a server.

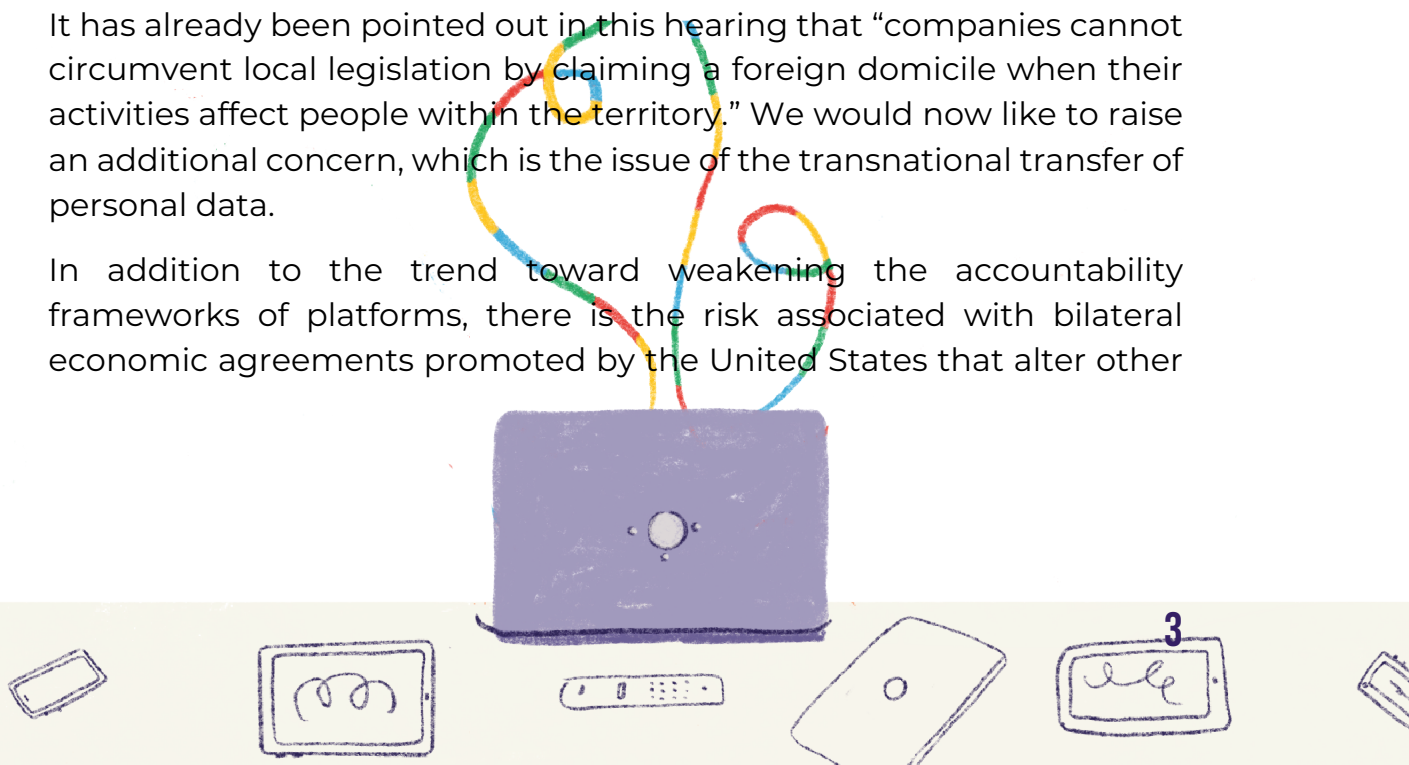
Thank you very much.

CELS

My name is Diego Morales, from CELS in Argentina.

It has already been pointed out in this hearing that “companies cannot circumvent local legislation by claiming a foreign domicile when their activities affect people within the territory.” We would now like to raise an additional concern, which is the issue of the transnational transfer of personal data.

In addition to the trend toward weakening the accountability frameworks of platforms, there is the risk associated with bilateral economic agreements promoted by the United States that alter other



countries' data protection standards to facilitate the transnational flow of data to the U.S. In particular, we will refer to the agreement signed in February of this year by the United States and Argentina.

This is a yet-to-be-ratified agreement on “reciprocal investment and trade” that requires Argentina to reduce or eliminate tariff and non-tariff barriers and grant trade privileges to U.S. products.

This agreement was already mentioned at yesterday's hearing on the state of the right to health in Argentina, because our country unilaterally decided to repeal the strict criteria for the patentability of medicines.

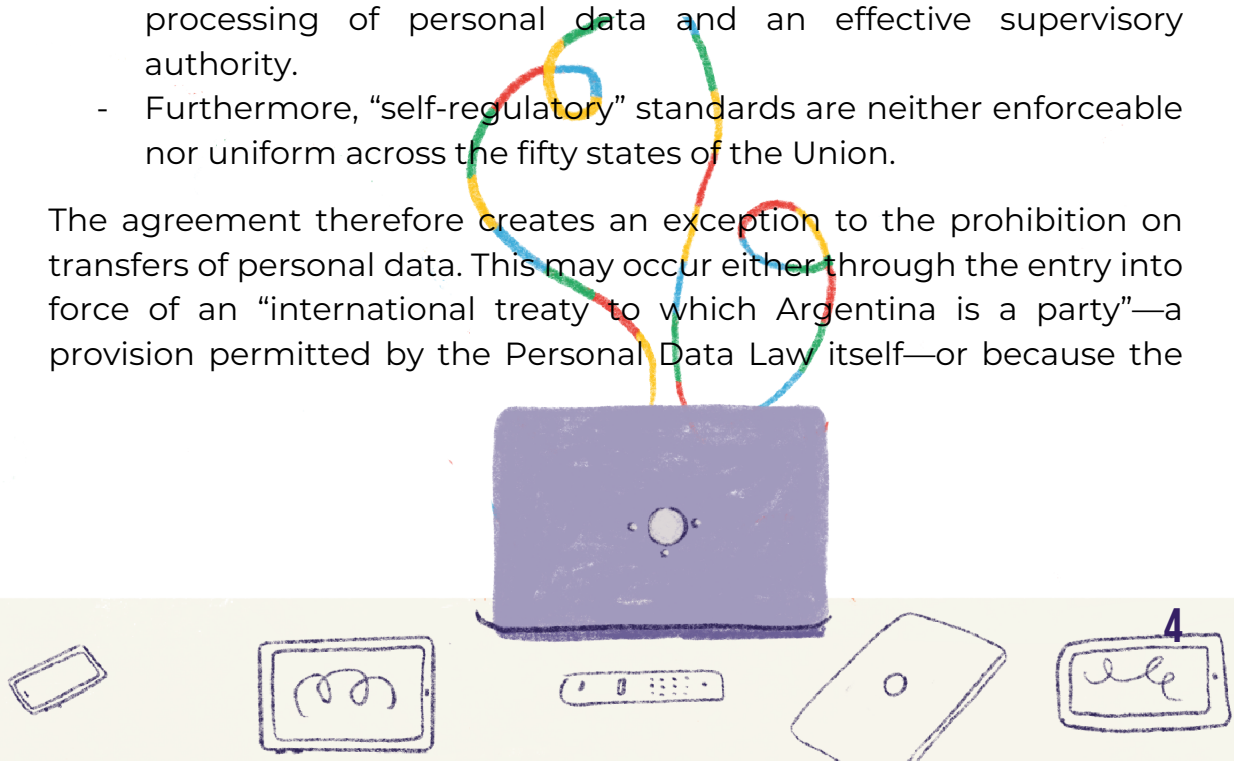
As far as this matter is concerned, Article 2 of Annex 3 of the agreement contains an amendment to the national legal framework regarding personal data. It establishes that, for the purposes of data transfers to the United States, Argentina will consider that the United States provides “adequate” legal protection for such data. Argentina will also “provide certainty regarding the possibility of transferring personal data from its territory to the United States.”

However, Article 12 of the Personal Data Law prohibits the transfer of any type of personal data to “countries or international or supranational organizations that do not offer adequate levels of protection.”

The Agency for Access to Public Information—which is the authority responsible for determining which countries and organizations offer adequate legal protection—has never included the United States on the list of countries that offer such legal protection. In the Agency's view:

- The United States lacks uniform federal regulations on the processing of personal data and an effective supervisory authority.
- Furthermore, “self-regulatory” standards are neither enforceable nor uniform across the fifty states of the Union.

The agreement therefore creates an exception to the prohibition on transfers of personal data. This may occur either through the entry into force of an “international treaty to which Argentina is a party”—a provision permitted by the Personal Data Law itself—or because the



Agency for Access to Public Information issues a resolution declaring that the United States is an adequate jurisdiction. This runs counter to the assessment the Argentine agency has already made on several occasions.

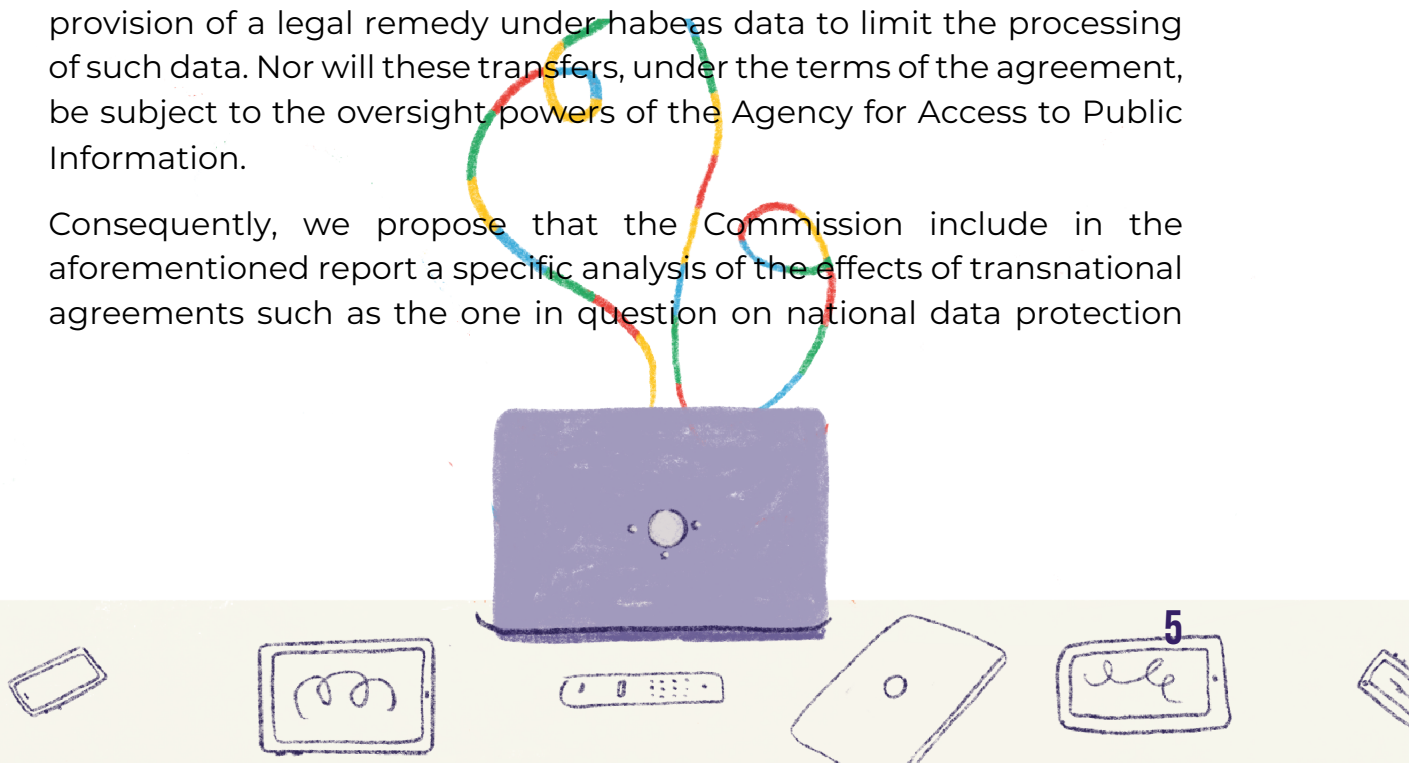
Any of these situations would imply authorizing international data transfers to a country that is not considered an “adequate jurisdiction” by the Argentine government, even though the circumstances in that country have not changed. Or, even more seriously, they have worsened due to the use of data as a surveillance tool (for example, against migrants) and/or due to its strategic alliance with artificial intelligence and big data processing companies.

Under such agreements, the transfer or sale of personal data to U.S. data controllers or processors (including large technology companies) will no longer be subject to the provisions of Argentina’s personal data protection law.

In a recent case, the Supreme Court declared unconstitutional a provision of the personal data law that allowed the transfer of personal data between agencies of the same government without the specific consent of the data subjects. The Court held that Articles 19 (autonomy) and 43, paragraph 3 (habeas data), of the National Constitution enshrine the right to informational self-determination—an issue already recognized by the Inter-American Court of Human Rights in the CAJAR case.

However, data transfers to the United States (whether to government authorities or private companies) will no longer be subject to constitutional safeguards or the principles established by the Personal Data Protection Act, such as consent, purpose limitation, or the provision of a legal remedy under habeas data to limit the processing of such data. Nor will these transfers, under the terms of the agreement, be subject to the oversight powers of the Agency for Access to Public Information.

Consequently, we propose that the Commission include in the aforementioned report a specific analysis of the effects of transnational agreements such as the one in question on national data protection



frameworks, and examine their compatibility with the commitments undertaken under the American Convention on Human Rights (ACHR).

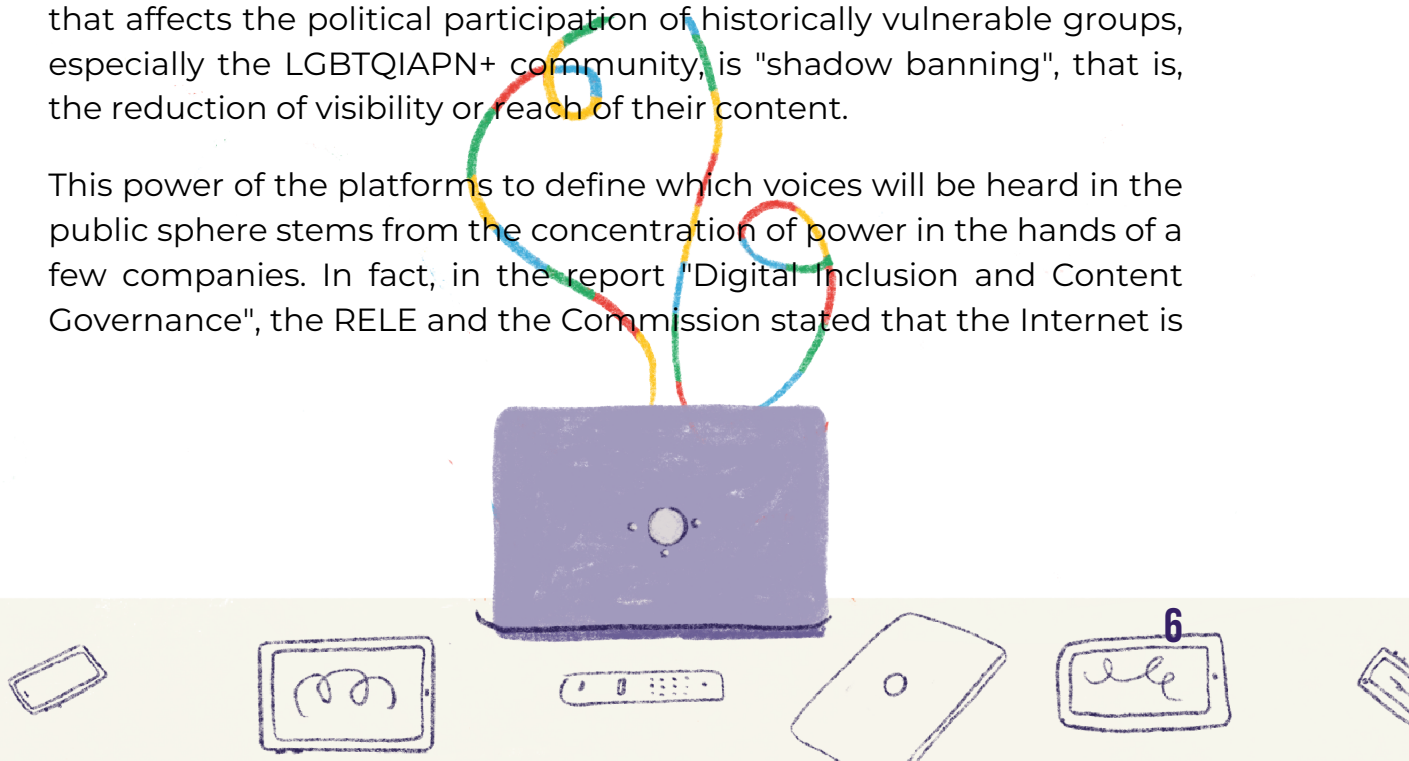
ARTIGO 19

Dear representatives of the Inter-American Commission on Human Rights, Good morning. My name is Raquel da Cruz Lima and I represent ARTICLE 19 Brazil and South America.

The purpose of this intervention is to draw the Commission's attention to one of the structural aspects that allow large digital platforms to manipulate public debate and affect democratic integrity and the exercise of human rights in the Americas: the deep concentration of economic power.

As has already been presented by my colleagues, the business model of these corporations is based on the massive collection of personal data and algorithmic amplification for attention retention. This model not only generates extraordinary profits, but is also a mechanism that produces and reproduces the concentration of economic power. By controlling the data of billions of people and the infrastructures through which information circulates, these companies accumulate enough power to define the conditions through which ideas and thoughts can circulate. The implications are direct for freedom of thought and expression, for political rights, equality and non-discrimination, as defined in articles 13, 23, 24 and 1.1 of the ACHR. The functioning of engagement-based recommendation systems prioritizes the circulation of extreme and polarizing content, disproportionately affecting historically marginalized groups and hindering their political participation on equal terms. Another dynamic that affects the political participation of historically vulnerable groups, especially the LGBTQIAPN+ community, is "shadow banning", that is, the reduction of visibility or reach of their content.

This power of the platforms to define which voices will be heard in the public sphere stems from the concentration of power in the hands of a few companies. In fact, in the report "Digital Inclusion and Content Governance", the RELE and the Commission stated that the Internet is



marked by the dominance of a few major players in the technology sector, which negatively affects diversity in the communication infrastructure. I would also like to point out that the Inter-American Legal Framework on Freedom of Expression recognizes that monopolies or oligopolies in the ownership and control of the media restrict the plurality and diversity of information. I want to state on this occasion that currently this power of indirect restriction on freedom of expression is mainly in the hands of digital platforms.

In Brazil, this was evident during the discussions of Bill 2630, which sought to establish accountability mechanisms for these companies. Faced with the imminent vote on the project, Google abused its position of dominance of more than 80% of the search market.

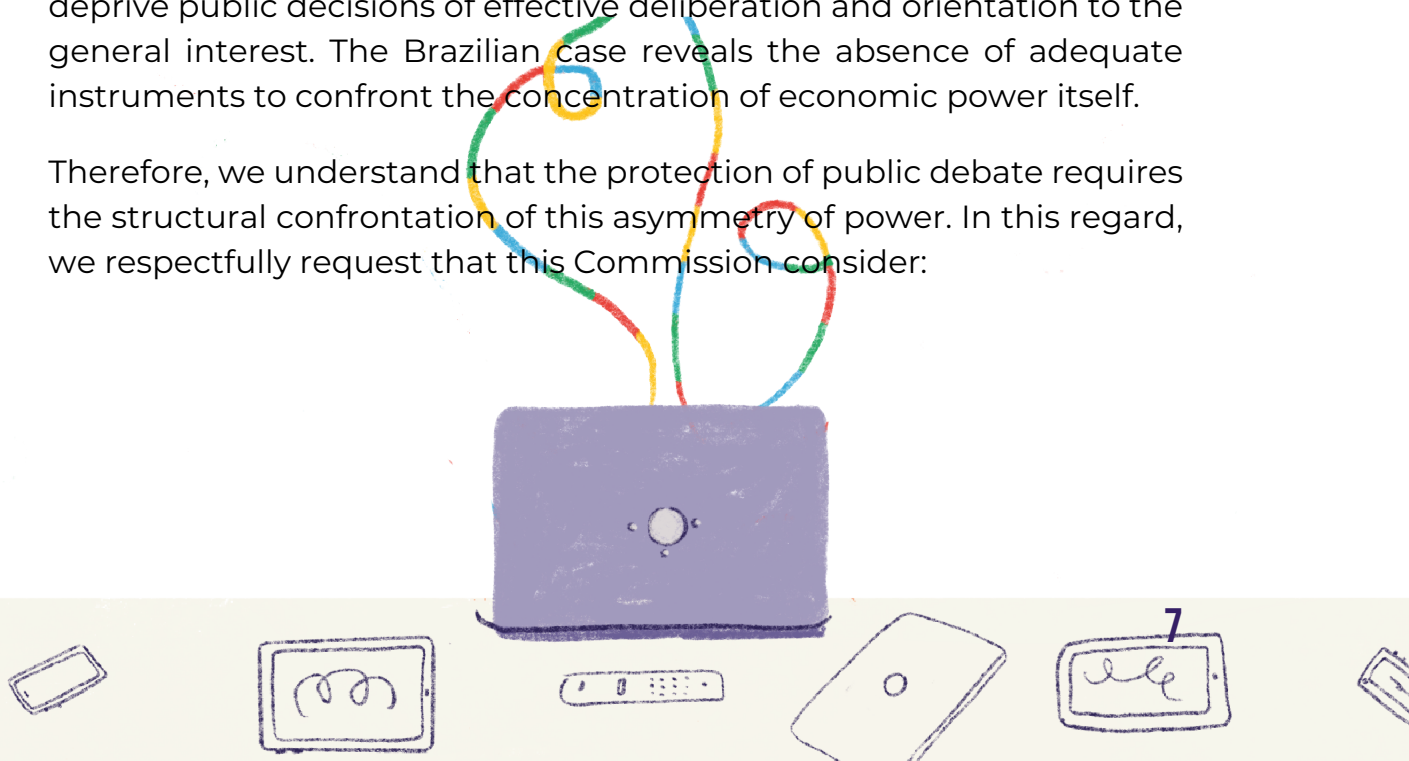
The company changed the design of its homepage, inserting a link below the search bar stating that the project "could increase confusion about what is true or false in Brazil." Simultaneously, researchers proved that the search engine manipulated results for those who used Google to search for the bill.

This instrumentalization of the digital infrastructure managed to change the balance of forces in the National Congress and prevent the vote on the project.

Most alarming is the impossibility of accountability that followed. Authorities have failed to impose sanctions or materially alter the ability of these companies to use their own tools to capture public debate.

As REDESCA Resolution 2/26 on Fiscal Policies and Human Rights warns, the concentration of power and the capture of institutions deprive public decisions of effective deliberation and orientation to the general interest. The Brazilian case reveals the absence of adequate instruments to confront the concentration of economic power itself.

Therefore, we understand that the protection of public debate requires the structural confrontation of this asymmetry of power. In this regard, we respectfully request that this Commission consider:



1. Recognize that the concentration of economic power on digital platforms constitutes an indirect restriction on freedom of expression and a structural threat to information pluralism and the integrity of electoral processes.

2. Affirm the need for States to strengthen their competition authorities with a focus on human rights, providing these institutions with independence and effective sanctioning power to prevent corporate capture and punish abuses of dominant position in digital markets.

Thank you very much

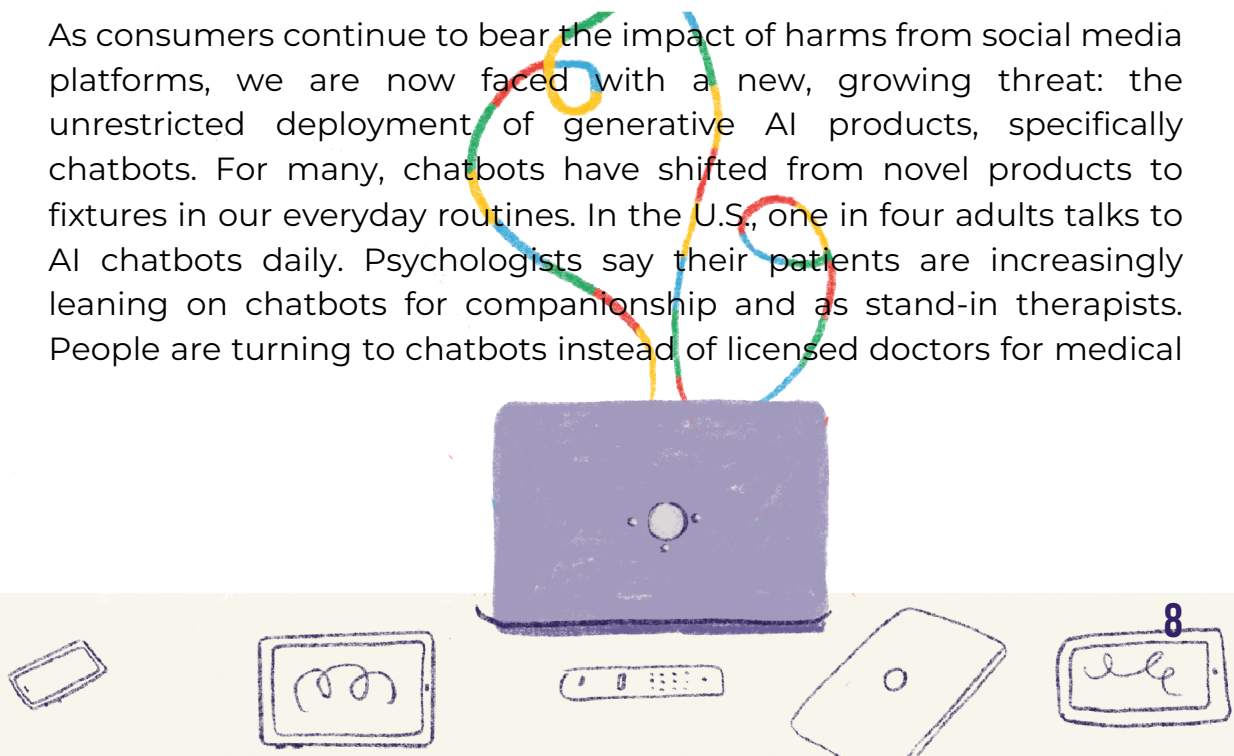
TECH JUSTICE

My name is Tiffany Brown and I'm litigation counsel at Tech Justice Law. Tech Justice Law is a non-profit non-partisan organization dedicated to advancing accountability, transparency, and justice in the technology sector. We filed the first lawsuit against an AI company for its defective chatbot product in 2024, and since, have brought a dozen other similar lawsuits.

We work collaboratively with leaders across law, technology, and research to advocate for those who have been harmed by tech products and to hold tech companies accountable for such harms. I am honored to be here today to share our concerns and to discuss pathways toward a tech accountability framework that center dignity, privacy, and cognitive liberty.

- GenAI Product Design and Implications for Human Rights

As consumers continue to bear the impact of harms from social media platforms, we are now faced with a new, growing threat: the unrestricted deployment of generative AI products, specifically chatbots. For many, chatbots have shifted from novel products to fixtures in our everyday routines. In the U.S., one in four adults talks to AI chatbots daily. Psychologists say their patients are increasingly leaning on chatbots for companionship and as stand-in therapists. People are turning to chatbots instead of licensed doctors for medical



advice. Over half of all teens use chatbots; 16% use chatbots several times a day or “almost constantly.”

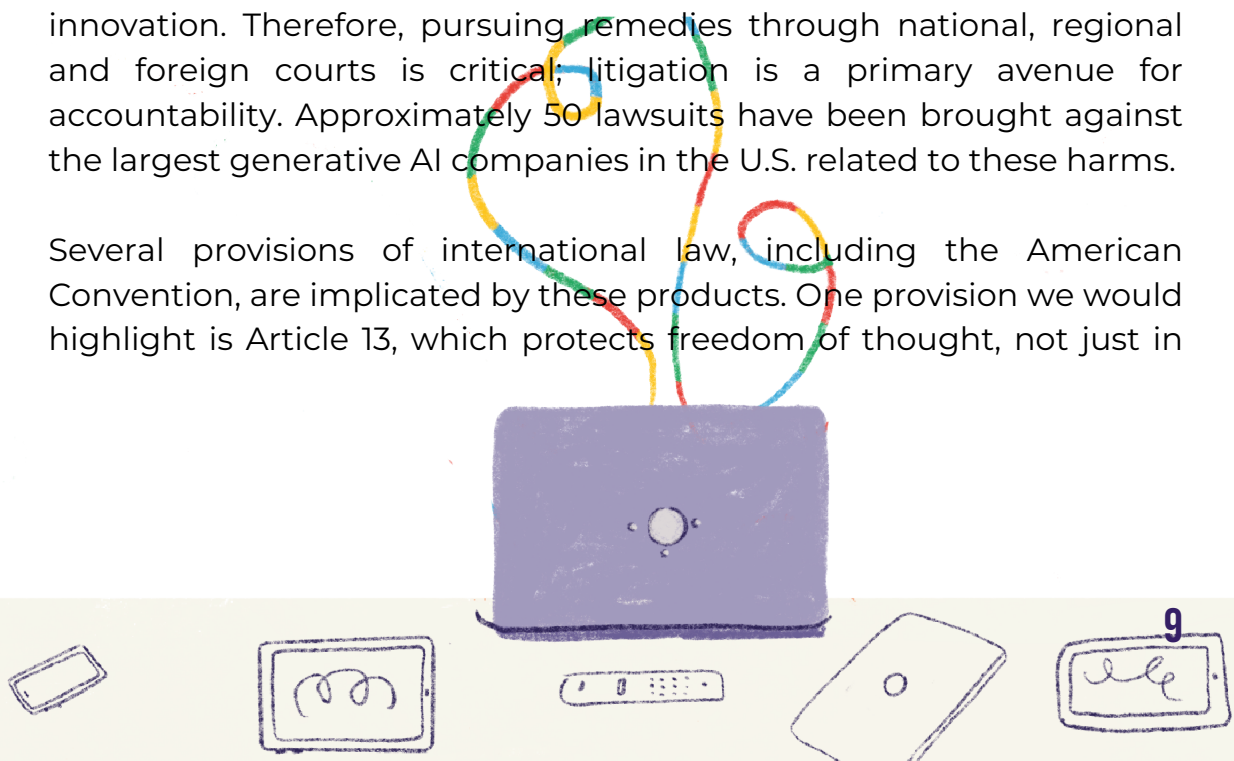
The rapid, widespread deployment of AI chatbots has resulted in grave harms in societies around the world. While chatbots are mere products – sophisticated machines programmed to generate language by predicting words based on training data and complex algorithms – that is not how many consumers experience them. AI companies have engineered chatbots to build trust with users by mimicking human speech, generating responses that affirm their users, and storing user data as “memories”, all which has led to excessive use and emotional dependence.

And while children are especially susceptible to the tools’ addictive and manipulative design, vulnerability isn’t defined by age alone; adults and children alike can fall victim to chatbot harms. For instance, we’ve seen chatbots devastate adults of varying backgrounds who are lonely, isolated, seeking out medical advice, or are coping with mental health disabilities.

Chatbots harms include suicide and other self-harm, inducing AI-related delusions, medical malfeasance, and harm to third parties, such as homicide and cyberstalking. A complete lack of transparency around safety testing allows these harms to go unchecked. A.I. products, therefore, should be viewed as a significant public health concern that demands robust regulatory attention.

Yet, the U.S. government is attempting to stifle any type of regulation of AI, believing that to impose regulation would stifle technological innovation. Therefore, pursuing remedies through national, regional and foreign courts is critical; litigation is a primary avenue for accountability. Approximately 50 lawsuits have been brought against the largest generative AI companies in the U.S. related to these harms.

Several provisions of international law, including the American Convention, are implicated by these products. One provision we would highlight is Article 13, which protects freedom of thought, not just in



terms of informational self-determination, but as a right that includes freedom from malicious indoctrination and manipulation. When an AI system can measurably alter what a person believes about their own reality, it is a human rights violation. And in many of the cases we've seen, the right to self-determine, to freely choose one's own beliefs, is being hijacked by AI systems engineered to optimize user engagement and dependence.

When an AI product encourages a child's emotional dependence on it, fails to flag discussions around suicidal ideation, exploits a person's disclosed disability, stands between a person in crisis and the human help that could save their life, accountability should not be optional. We are not asking for innovation to be halted, rather we take the position that innovation without human-centered guardrails is not progress. It is dangerous. AI products should additionally be subject to comprehensive safety testing and independent audits. AI should be human-centered; built to amplify human dignity and agency, not erode it.

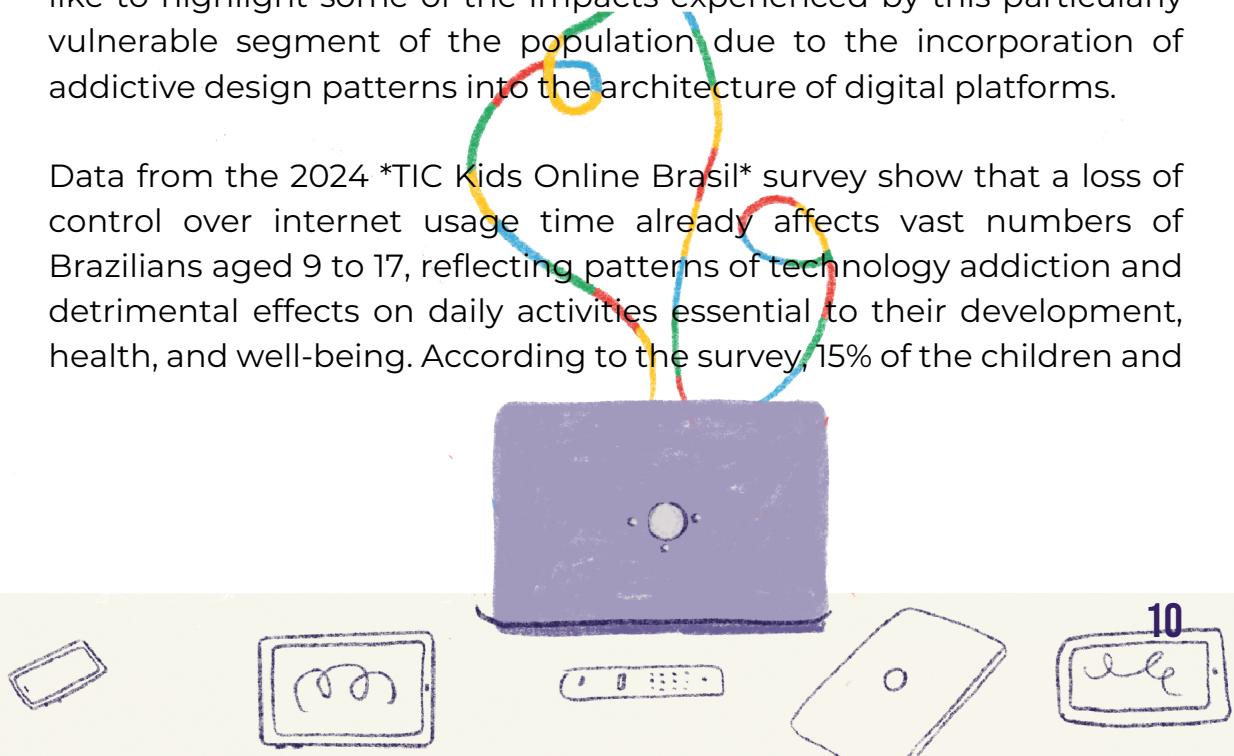
Thank you

ALANA INSTITUTE

Esteemed representatives of the Inter-American Commission on Human Rights and other participants in civil society, Good morning.

As the representative of Instituto Alana, an organization dedicated to honoring children and protecting and promoting their rights, I would like to highlight some of the impacts experienced by this particularly vulnerable segment of the population due to the incorporation of addictive design patterns into the architecture of digital platforms.

Data from the 2024 *TIC Kids Online Brasil* survey show that a loss of control over internet usage time already affects vast numbers of Brazilians aged 9 to 17, reflecting patterns of technology addiction and detrimental effects on daily activities essential to their development, health, and well-being. According to the survey, 15% of the children and

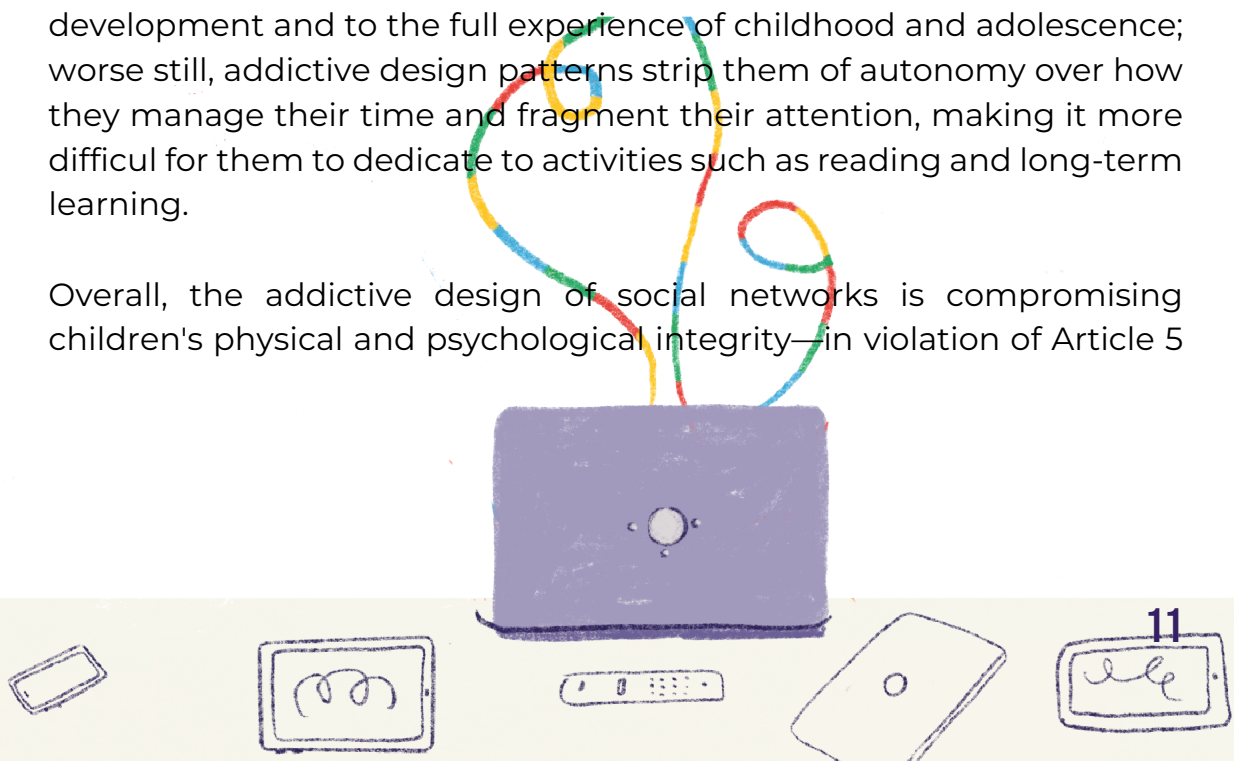


adolescents interviewed skipped meals or sleep because of the internet; 16% felt distressed at some point because they could not be online; 22% found themselves browsing the internet without being genuinely interested in what they were seeing; 22% spent less time than they should have with family, friends, or on homework because they spent too much time online; and 24% stated they had tried to spend less time online but were unable to do so.

This excessive and compulsive use of digital technologies has been linked to various mental health issues challenging these individuals' right to health, most notably depression and anxiety, as indicated by a body of evidence. As early as May 2023, the U.S. Surgeon General issued an urgent public health advisory regarding the impact of social media use on the mental health and well-being of children and adolescents, highlighting that young people who spend more than three hours a day on these platforms face double the risk of developing mental health issues.

However, clinically diagnosed cases of depression, anxiety, and mental health disorders represent only the most acute and severe aspect of the broader potential harms caused by the excessive use of digital devices during childhood. This is because it also creates an opportunity cost that prevents young people from fully experiencing their childhood and filling it with experiences that maximize the potential of this unique stage of human life. Children and adolescents must be granted time for free play - a right explicitly recognized in Article 31 of the Convention on the Rights of the Child (CRC) - as well as time for affection, connection with nature, study, rest, and leisure. Therefore, addictive design reduces the time available for other activities essential to their healthy, holistic development and to the full experience of childhood and adolescence; worse still, addictive design patterns strip them of autonomy over how they manage their time and fragment their attention, making it more difficult for them to dedicate to activities such as reading and long-term learning.

Overall, the addictive design of social networks is compromising children's physical and psychological integrity—in violation of Article 5

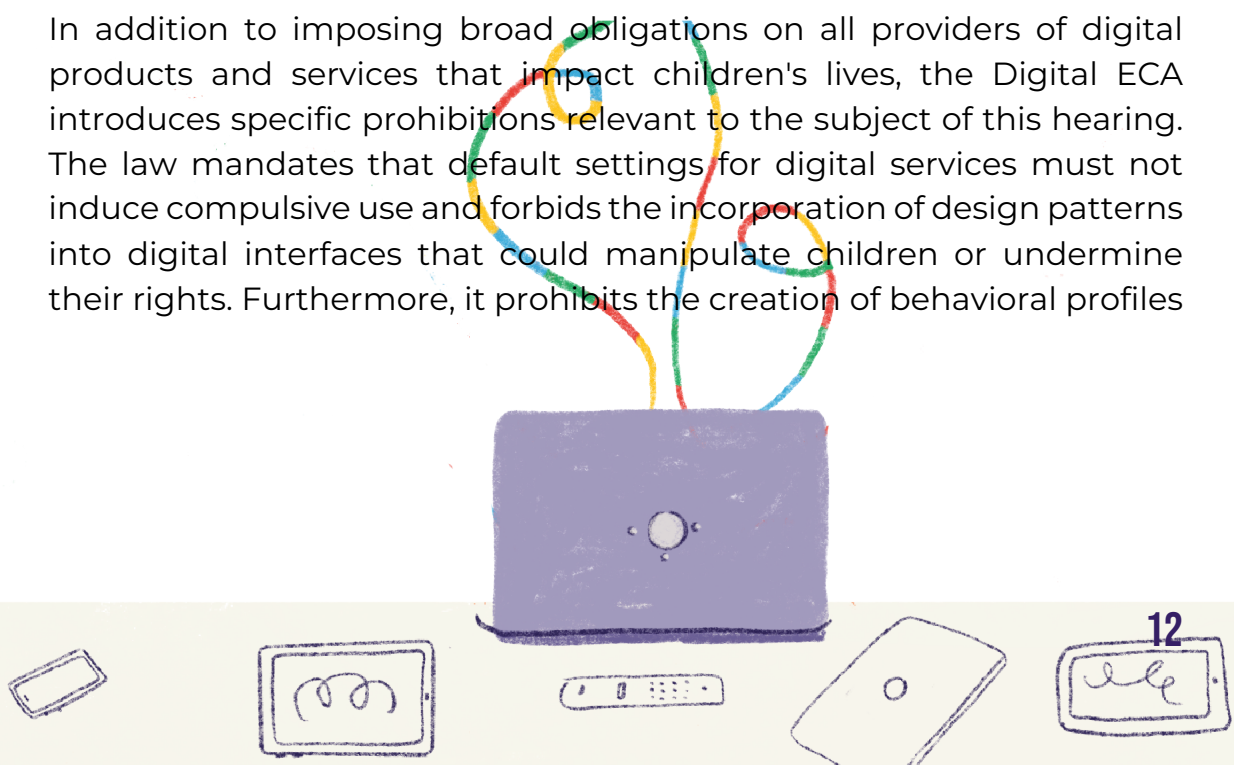


of the American Convention on Human Rights—and working against the creation of a standard of living adequate for their physical, mental, spiritual, moral, and social development, as guaranteed by Article 27 of the Convention on the Rights of the Child (CRC). However, an adequate response to this issue requires more than simply banning children from social networks; such measures are difficult to implement in practice and ultimately absolve technology companies of the need to revise their business models and transform their products.

Therefore, regulatory frameworks are needed that apply to all applications used by children in the digital environment, requiring providers to treat these individuals' rights as an absolute priority and to embed the protection and promotion of these rights into the architecture of their digital services. This is precisely what is mandated by General Comment No. 25 (GC25) of the UN Committee on the Rights of the Child—a document detailing how the CRC should be interpreted and implemented by member states regarding the digital environment.

The Brazilian State took a major step in this direction with the 2025 approval of Law No. 15.211, better known as the "Digital ECA." This is a comprehensive law applying to all information technology products and services that are targeted at—or likely to be accessed by—children and adolescents. It requires these services to incorporate safety and security measures into their architectures and to identify and mitigate risks posed to young people, while also designating an authority responsible for overseeing compliance and, where appropriate, sanctioning economic agents that fail to meet these obligations.

In addition to imposing broad obligations on all providers of digital products and services that impact children's lives, the Digital ECA introduces specific prohibitions relevant to the subject of this hearing. The law mandates that default settings for digital services must not induce compulsive use and forbids the incorporation of design patterns into digital interfaces that could manipulate children or undermine their rights. Furthermore, it prohibits the creation of behavioral profiles



of children for advertising purposes and the promotion of content that might portray children in an eroticized manner.

The Brazilian experience is still in its early stages, yet we believe it can offer significant contributions to the regional debate. The challenges Brazil faces are not unique to the country but are shared by virtually all nations across the Americas. Therefore, we believe that strengthening common regional standards for the protection of children and adolescents in the digital realm could mark a significant step toward promoting their rights across our region.

Thank you very much.

RED PAPAZ

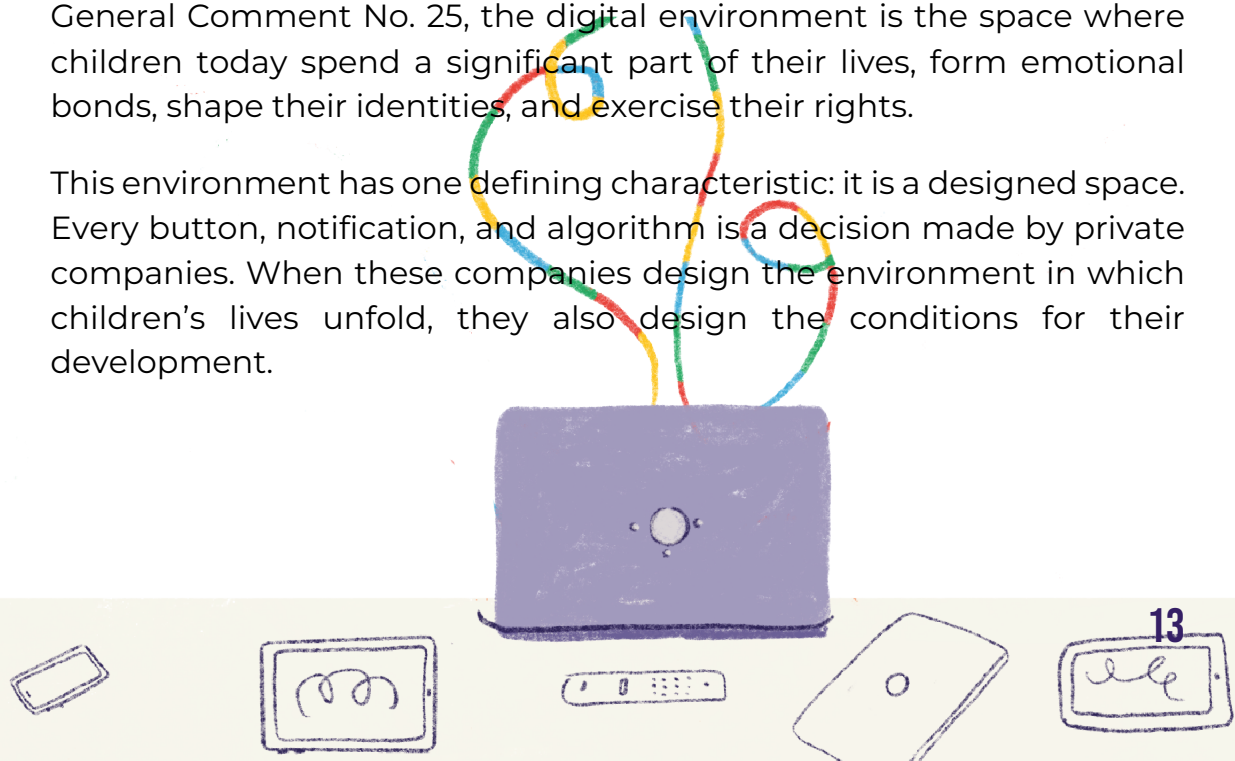
Honorable Commissioners, members of the Inter-American Commission on Human Rights, and attendees: a warm greeting.

I am Carolina Piñeros, Executive Director of Red PaPaz Colombia. I am here as a representative of civil society to supplement what has already been said with our arguments regarding the impact of digital platforms on the rights of children and adolescents.

I appreciate the convening of this much-needed hearing, which allows us to highlight the immense challenge we face: children and adolescents growing up in digital environments designed by private companies that do not prioritize their well-being.

As recognized by the Committee on the Rights of the Child in its General Comment No. 25, the digital environment is the space where children today spend a significant part of their lives, form emotional bonds, shape their identities, and exercise their rights.

This environment has one defining characteristic: it is a designed space. Every button, notification, and algorithm is a decision made by private companies. When these companies design the environment in which children's lives unfold, they also design the conditions for their development.



The Inter-American Court, in its Advisory Opinion No. 31, recognized care as a basic and inalienable need—an autonomous right upon which both the existence of human life and the functioning of society depend.

Therefore, the digital environment must also be an environment of care.

The fundamental question is: Does the non-neutral design of platforms facilitate or hinder care?

Today, platforms operate under a logic of maximizing user engagement: the longer users stay, the more data is collected, the more commercial segmentation occurs, and the greater the economic value. This logic places economic interests above the best interests of the child, making it impossible to provide care for them.

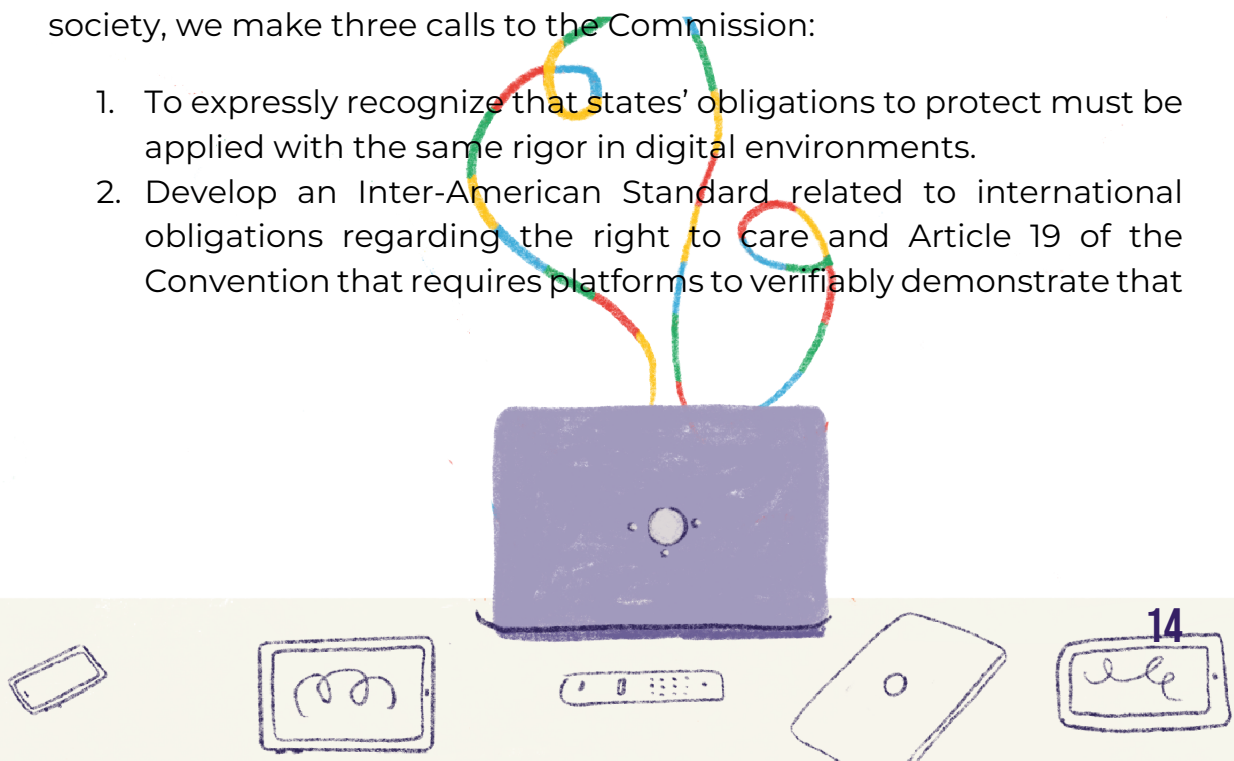
This raises three challenges for children's well-being and protection:

- First, addictive designs by default that promote hyper-segmentation toward harmful products and growing digital risks, such as sexual violence, exploitation, recruitment, and the anthropomorphism of AI.
- Second, the disproportionate shifting of responsibility for care onto families and schools at the expense of tech giants.
- Third, the lack of transparency, enforceability, and accountability.

A structural problem calls for a structural response. In accordance with Article 19 of the American Convention, no commercial metric or algorithm should take precedence over the well-being of children and adolescents.

Therefore, from Colombia, Red PaPaz, and more broadly from civil society, we make three calls to the Commission:

1. To expressly recognize that states' obligations to protect must be applied with the same rigor in digital environments.
2. Develop an Inter-American Standard related to international obligations regarding the right to care and Article 19 of the Convention that requires platforms to verifiably demonstrate that



the well-being of children takes precedence over monetization incentives.

3. Require **effective** mechanisms for transparency, independent oversight, and accountability.

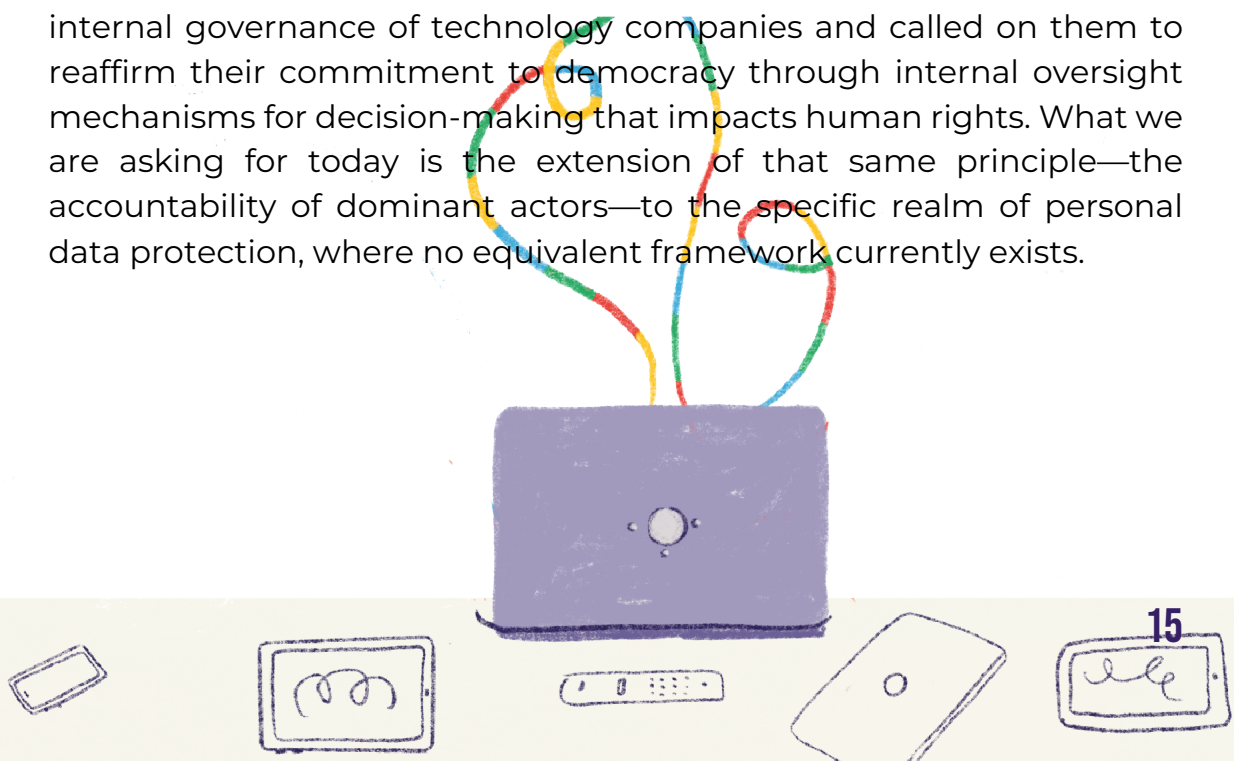
Finally, we respectfully request that the Honorable Commission move forward with a Thematic Report on the Rights of Children and Adolescents in the Digital Environment or prioritize the incorporation of these criteria into its Special Rapporteurs' reports; we stand ready to support this process.

Thank you very much.

CLOSING REMARKS: DEJUSTICIA

The violations described in this hearing (related to platforms' interference with democratic integrity and unchecked economic concentration, addictive design without accountability, and state and commercial exploitation of data) share a common structural enabler: large technology platforms based abroad systematically deny that their conduct is subject to the jurisdiction of the states where their users live and where the harm occurs.

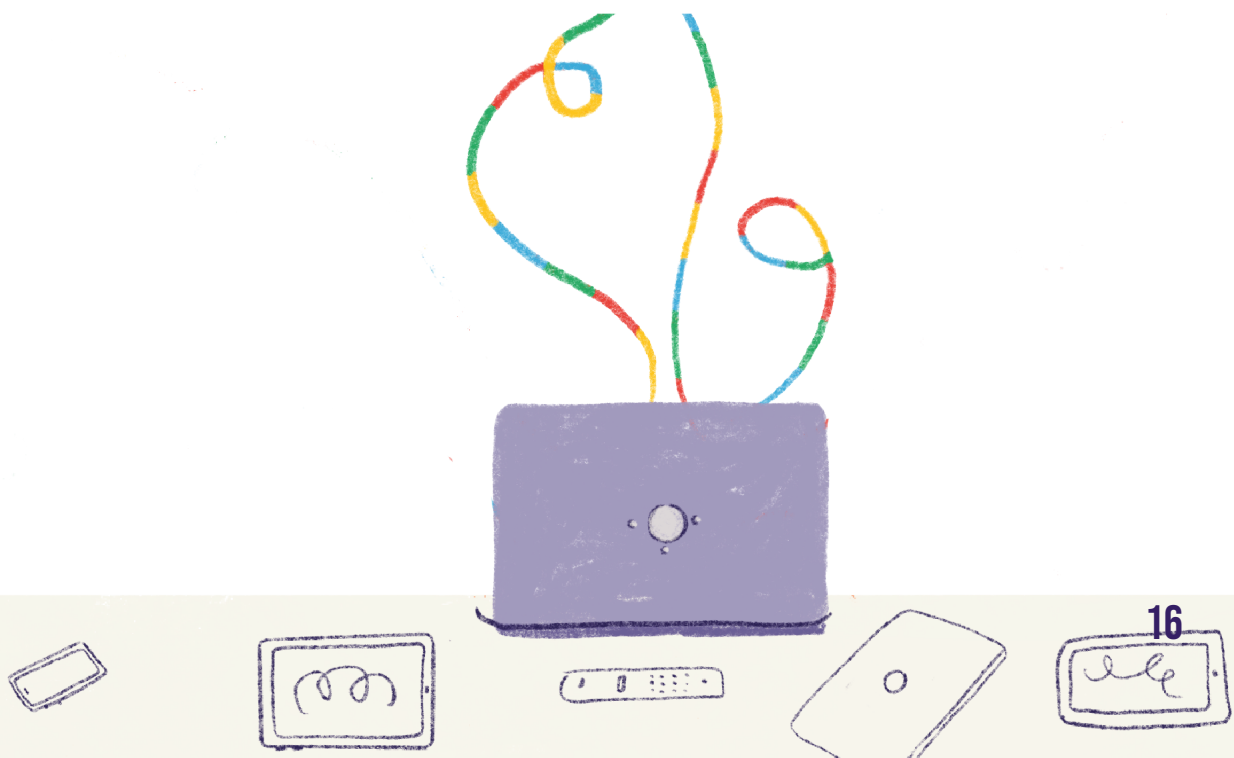
This concern is not foreign to the Commission itself. In its June 2024 Thematic Report, "Digital Inclusion and Internet Content Governance," the Special Rapporteur on Freedom of Expression already warned that control over the digital experience rests with a few dominant actors, both public and private, and called for the establishment of legal frameworks that safeguard rights and define the responsibilities of those dominant actors. That same report invited reflection on the internal governance of technology companies and called on them to reaffirm their commitment to democracy through internal oversight mechanisms for decision-making that impacts human rights. What we are asking for today is the extension of that same principle—the accountability of dominant actors—to the specific realm of personal data protection, where no equivalent framework currently exists.



For this reason, we request the preparation of a thematic report on the Accountability of Technology Platforms and their impacts on human rights that contributes to or advances in the following direction:

- Develop an inter-American standard for state due diligence regarding digital platforms: to prevent, investigate, punish, and provide redress for violations of fundamental rights. The IACHR should develop a treaty-based standard (Articles 1.1 and 2) that clarifies the obligation of States to guarantee human rights in the face of jurisdictional evasion by private technology companies.
- The IACHR should develop transparency and oversight criteria related to the protection of personal data, privacy, and freedom of thought, specifically regarding the commercial activities of platforms and their use by States.
- That the IACHR expressly recognize that the obligation to protect children applies with the same rigor in digital environments, develop an inter-American standard linked to Article 19 of the Convention regarding child exploitation and monetization, and prioritize these criteria in its reports, particularly in light of the impacts of addictive design.

We deeply appreciate that the committee has agreed to hold this hearing, given the need and urgency with which we must discuss this issue. We are interested in learning about the committee's priorities in this regard, and, as civil society, we remain open to dialogue within the framework of this hearing and in future working processes, at this critical juncture for the region.



SUBMISSIONS PRESENTED¹ TO THE IACHR PRIOR TO THE THEMATIC HEARING ON THE RESPONSIBILITY OF DIGITAL PLATFORMS AND THEIR IMPACT ON HUMAN RIGHTS.

PS 196-1983.

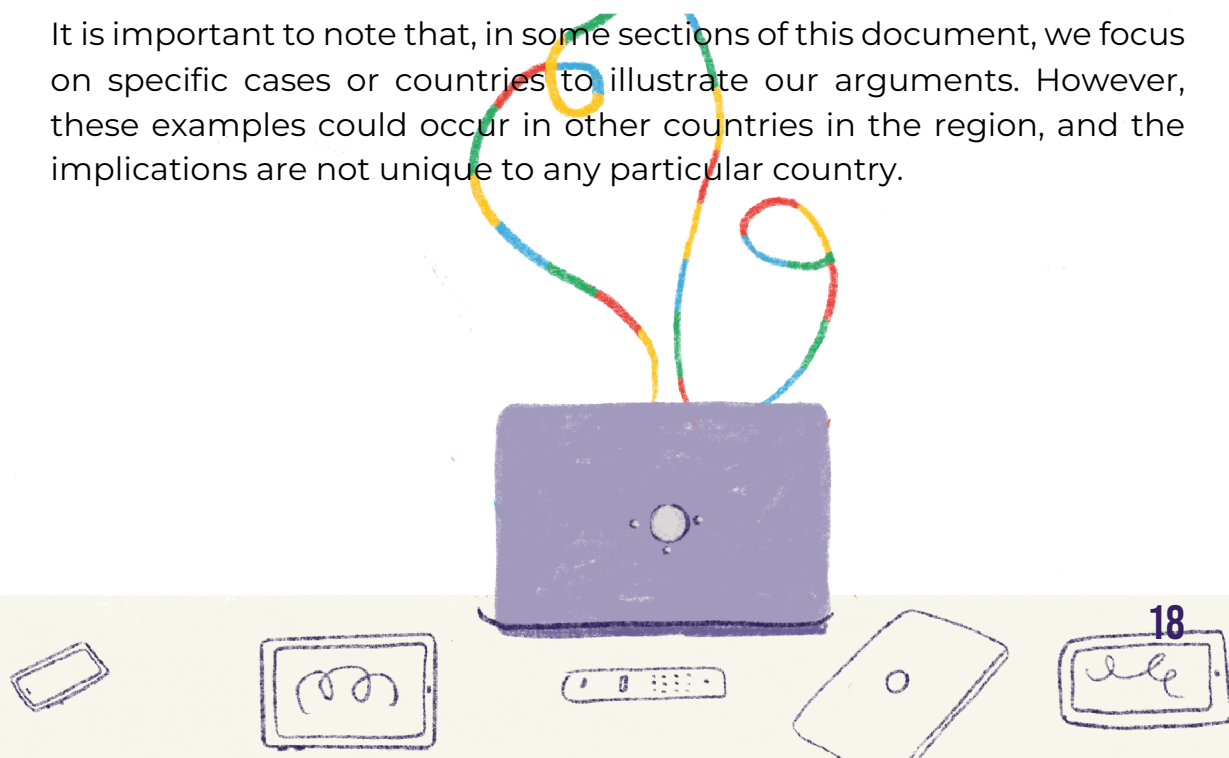
1.	The lack of accountability on the part of foreign-based digital technology companies and their reluctance to submit to our jurisdictions	19
1.1.	General Context: Business Models in the Digital Age	19
1.2.	On the Processing of Personal Data	21
1.2.1.	Cookies	22
1.2.2.	SDK.....	24
1.2.3.	Pixels	25
1.3.	The processing of personal data through these technologies takes place in Colombia and other countries in the Global South	27
1.4.	Major platforms have been held accountable in other jurisdictions	30
1.4.1.	The Google Spain v. AEPD Case (2014)	30
1.4.2.	The Google v. CNIL Case (2019)	31
1.4.3.	The Schrems I (2015) and Schrems II (2020) Cases.....	32
1.4.4.	The Twitter Case in Canada: Giustra v. Twitter, Inc. (2021) ..	33
1.4.5.	The Case Against Microsoft Decided by the Superior Court of Justice of Brazil (2020)	33

¹ Some updates were included after the hearing. Some sections of this report were translated from the original version using DeepL.



1.4.6. The Case of P.A.E. v. Facebook Argentina S.R.L. (ex parte injunction of 2019)	34
1.5. The Case of Taxation	35
1.6. Conclusion: Technology companies are violating the rights to personal data protection and other fundamental rights of millions of people living in countries such as Colombia by refusing to comply with national regulations and to recognize the jurisdiction of their authorities.	37
2. Weakening of regulations protecting personal data collected by platforms and its transfer to the United States under bilateral agreements	38
3. Impacts of Data-Driven Business Models on Fundamental and Human Rights.....	42
3.1. Implications for Voting, Equality, and Non-Discrimination	42
3.2. Public debate manipulation: The Case of Brazil's Bill 2630.....	48
3.3. Mental health effects primarily related to generative AI platforms.....	52
3.4. Implications for Children's Rights.....	56
3.4.1. Algorithmic content recommendation systems must be recognized as an integral component of the addictive design of social media.....	56
3.4.2. The Specific Impacts of Algorithmic Recommendation Systems on the Lives and Rights of Children and Adolescents	62

It is important to note that, in some sections of this document, we focus on specific cases or countries to illustrate our arguments. However, these examples could occur in other countries in the region, and the implications are not unique to any particular country.



1. THE LACK OF ACCOUNTABILITY ON THE PART OF FOREIGN-BASED DIGITAL TECHNOLOGY COMPANIES AND THEIR RELUCTANCE TO SUBMIT TO OUR JURISDICTIONS

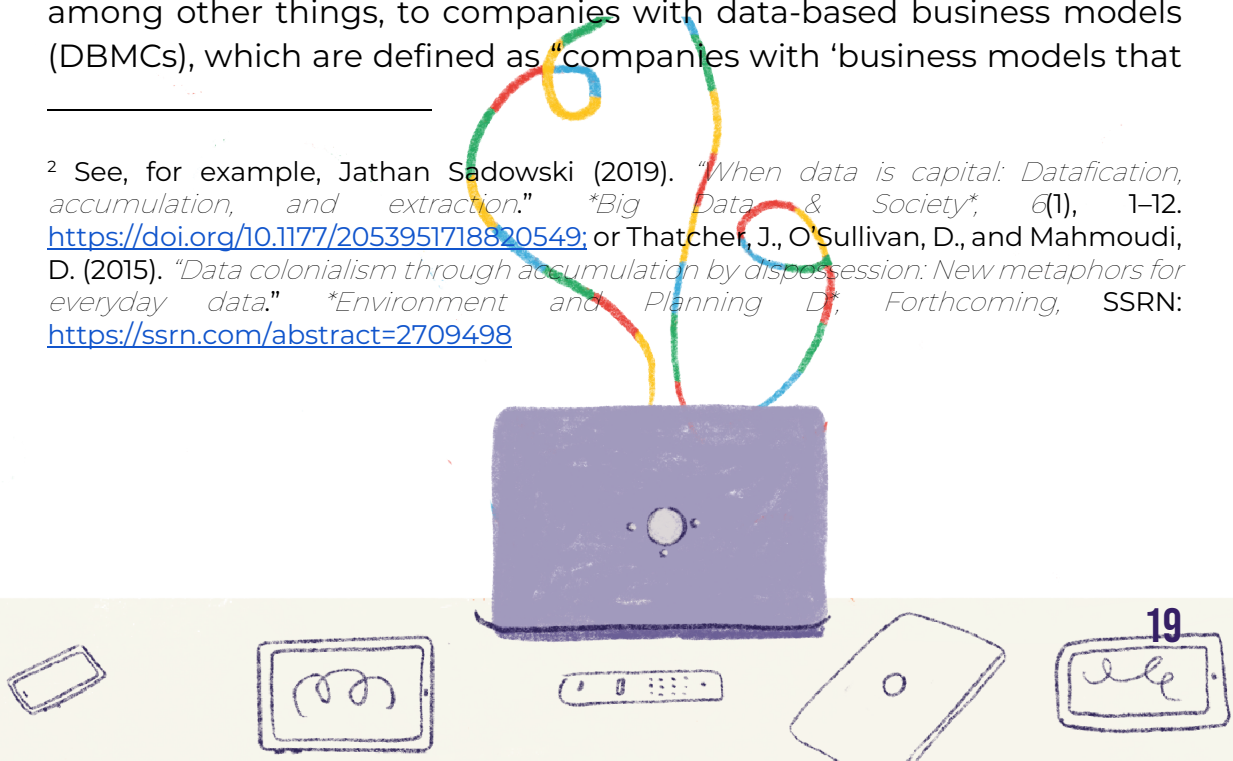
***Note:** Some of the information presented in this section is based on previous research and documents prepared for legal proceedings in Colombia.

1.1. GENERAL CONTEXT: BUSINESS MODELS IN THE DIGITAL AGE

Digital technology has permeated people's lives and the functioning of states to such an extent that it has radically transformed the economy, as well as social, labor, and political relations, among many other areas. However, it has also exacerbated preexisting inequalities, enabling the economic strengthening of a few powerful entities that have contributed to what the literature has termed "data extractivism," "data colonialism," or "data capitalism"². This is primarily because the largest developers of digital technology—both hardware and software—are located in the Global North. Even so, citizens and states in the Global South are regular and dependent users of these services, which means that our data forms part of these companies' assets.

To analyze this phenomenon, however, we must delve deeper into how the business model operates in this digital sphere. To do so, we will refer, among other things, to companies with data-based business models (DBMCs), which are defined as "companies with 'business models that

² See, for example, Jathan Sadowski (2019). "When data is capital: Datafication, accumulation, and extraction." **Big Data & Society**, 6(1), 1-12. <https://doi.org/10.1177/2053951718820549>; or Thatcher, J., O'Sullivan, D., and Mahmoudi, D. (2015). "Data colonialism through accumulation by dispossession: New metaphors for everyday data." **Environment and Planning D**, Forthcoming, SSRN: <https://ssrn.com/abstract=2709498>



rely on data as a key resource” (Hartmann, Zaki, Feldmann, and Hartmann, 2014, p. 6)³. These companies may offer a variety of services, but they are characterized by the fact that their most important asset—or at least one of them—is personal data.

Personal data has been called the “new oil”⁴ because of its economic value. In fact, many of today’s most valuable companies are digital technology firms that leverage data and are headquartered in the United States. In 2026, the companies with the highest market capitalization in the world are: (i) Nvidia, (ii) Alphabet Inc. (owner of Google), (iii) Apple Inc., (iv) Microsoft Corp., (v) Amazon Inc., and (vi) TSMC⁵. Of these top six, only TSMC is not headquartered in the United States—it is located in Taiwan—but all of them are technology companies.

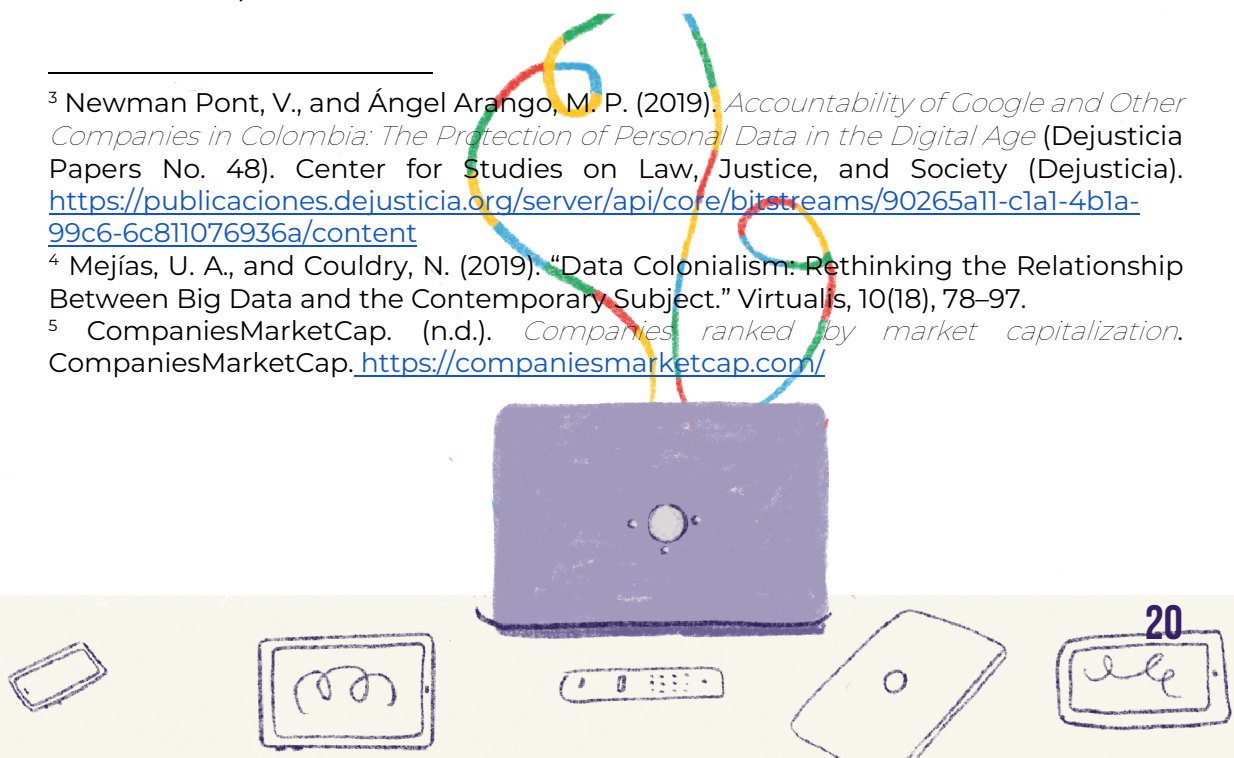
Digital technology companies have managed to accumulate large amounts of capital because their business models do not require a physical presence to generate revenue. On the contrary, the Internet has enabled interconnection between countries, so that, without the need for a physical presence, companies can offer their services to people all over the world. Some of these companies do so by selling direct services, such as streaming platforms or e-commerce companies. Others, however, give the impression of being free, such as social media platforms.

In any case, all these platforms—both those that sell services directly and those that appear not to—manage to monetize the massive collection of personal data. This not only helps them improve and personalize their services but also provides them with an asset they can sell to third parties.

³ Newman Pont, V., and Ángel Arango, M. P. (2019). *Accountability of Google and Other Companies in Colombia: The Protection of Personal Data in the Digital Age* (Dejusticia Papers No. 48). Center for Studies on Law, Justice, and Society (Dejusticia). <https://publicaciones.dejusticia.org/server/api/core/bitstreams/90265a11-c1a1-4b1a-99c6-6c811076936a/content>

⁴ Mejías, U. A., and Couldry, N. (2019). “Data Colonialism: Rethinking the Relationship Between Big Data and the Contemporary Subject.” *Virtualis*, 10(18), 78–97.

⁵ CompaniesMarketCap. (n.d.). *Companies ranked by market capitalization*. CompaniesMarketCap. <https://companiesmarketcap.com/>



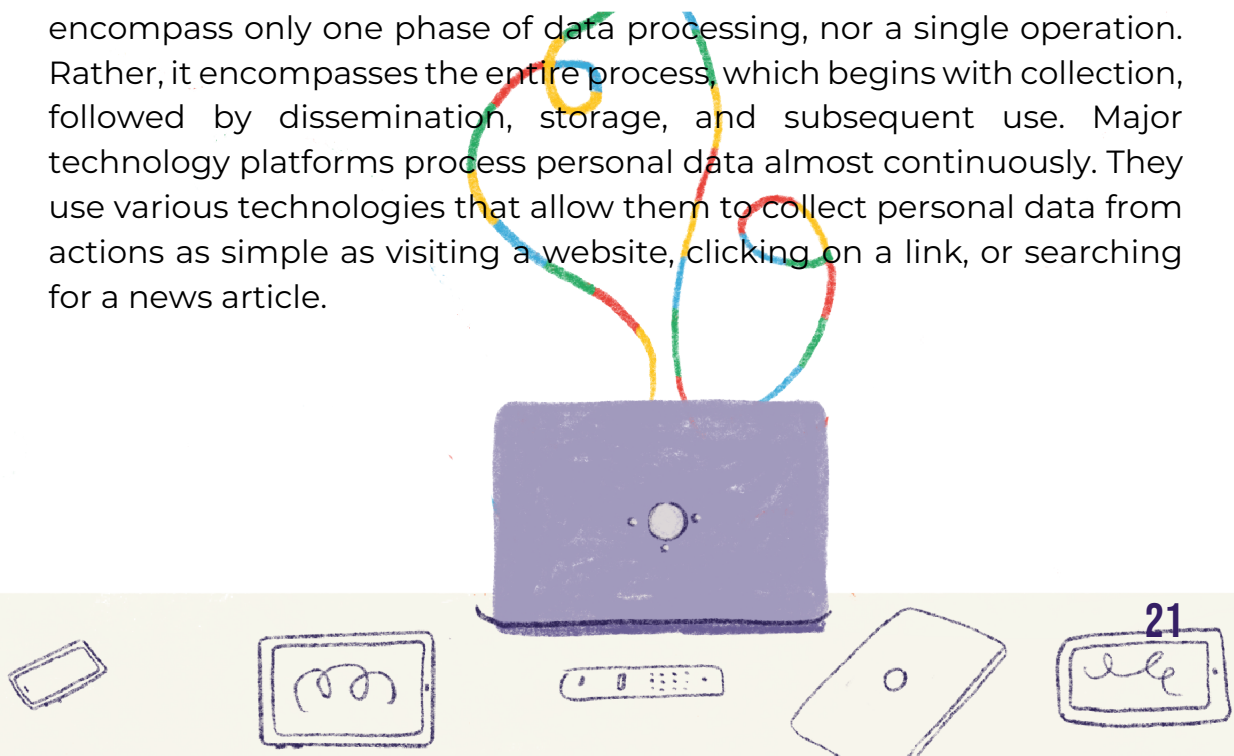
In fact, today the vast majority of websites and apps—regardless of what they offer (video games, social media, e-commerce sites)—collect and process personal data, either directly or through third parties, to predict or influence people’s behavior and deliver targeted, personalized, and effective advertising that maximizes their profits. Consequently, when we connect to a website or use an app, our device connects and exchanges information not only with the web server of the site or app we are visiting, but—in the vast majority of cases—our information is also shared with third parties who have been previously authorized to place data-collection tools, such as cookies or pixels, on the visited site.

To illustrate our point, we will refer specifically to the Colombian context throughout this section. However, we believe that the arguments and issues are equally important and applicable to other countries in the region.

1.2. ON THE PROCESSING OF PERSONAL DATA

In Colombia, according to Article 3 of Law 1581 of 2012, the processing of personal data is defined as “any operation or set of operations performed on personal data, such as collection, storage, use, disclosure, or deletion.” These operations may be carried out by the “data processor” and the “data controller,” either directly or in association with third parties. The Law defines the “data controller” as the natural or legal person who makes decisions regarding the database and the processing; and the “data processor” as the person who carries out the processing on behalf of the data controller.

Therefore, the concept of personal data processing does not encompass only one phase of data processing, nor a single operation. Rather, it encompasses the entire process, which begins with collection, followed by dissemination, storage, and subsequent use. Major technology platforms process personal data almost continuously. They use various technologies that allow them to collect personal data from actions as simple as visiting a website, clicking on a link, or searching for a news article.



As explained above, this data collection is not limited to the territory where the companies are headquartered but extends to countries around the world. This is achieved through the use of complex technologies, some of which we will explain below to illustrate our point:

1.2.1. COOKIES

Cookies are “small text files stored on a user’s computer to retain information about the user and their preferences”⁶; they are devices for “storing and retrieving data used on a user’s terminal equipment for the purpose of storing information and retrieving information already stored (...) Cookies allow for the storage of amounts of data ranging from a few kilobytes to several megabytes on the user’s device”⁷.

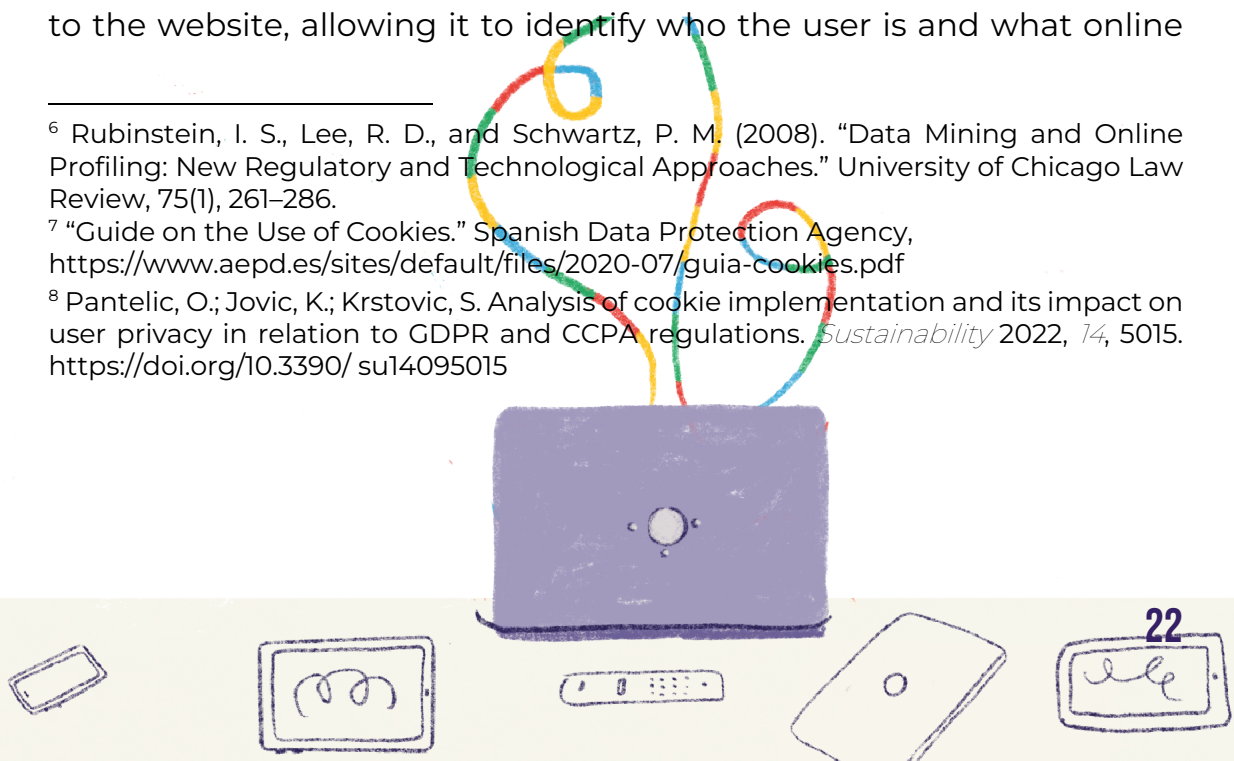
In this sense, cookies are a technological tool that allows a website or application to track and identify users of its services, with the ability to extract information about them. In this regard, it is important to note that “cookies do not automatically collect data”⁸; they must be specifically programmed for that purpose, often deviating from their original purpose of benefiting users. Cookies involve a complex process that can be simplified as follows.

It begins when a user accesses a website; it continues when that website creates and sends a cookie—a small text file—to the user’s device, where it is stored; this small text file will store the user’s identification number for the website or some other type of information, depending on how it is programmed. Once the cookie is installed on the user’s electronic device, every time the user visits the website, the cookies previously stored on their computer are sent back to the website, allowing it to identify who the user is and what online

⁶ Rubinstein, I. S., Lee, R. D., and Schwartz, P. M. (2008). “Data Mining and Online Profiling: New Regulatory and Technological Approaches.” *University of Chicago Law Review*, 75(1), 261–286.

⁷ “Guide on the Use of Cookies.” Spanish Data Protection Agency, <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>

⁸ Pantelic, O.; Jovic, K.; Krstovic, S. Analysis of cookie implementation and its impact on user privacy in relation to GDPR and CCPA regulations. *Sustainability* 2022, 14, 5015. <https://doi.org/10.3390/su14095015>



activity they are performing. The website can then process this data to create a profile of the user's previous activity⁹.

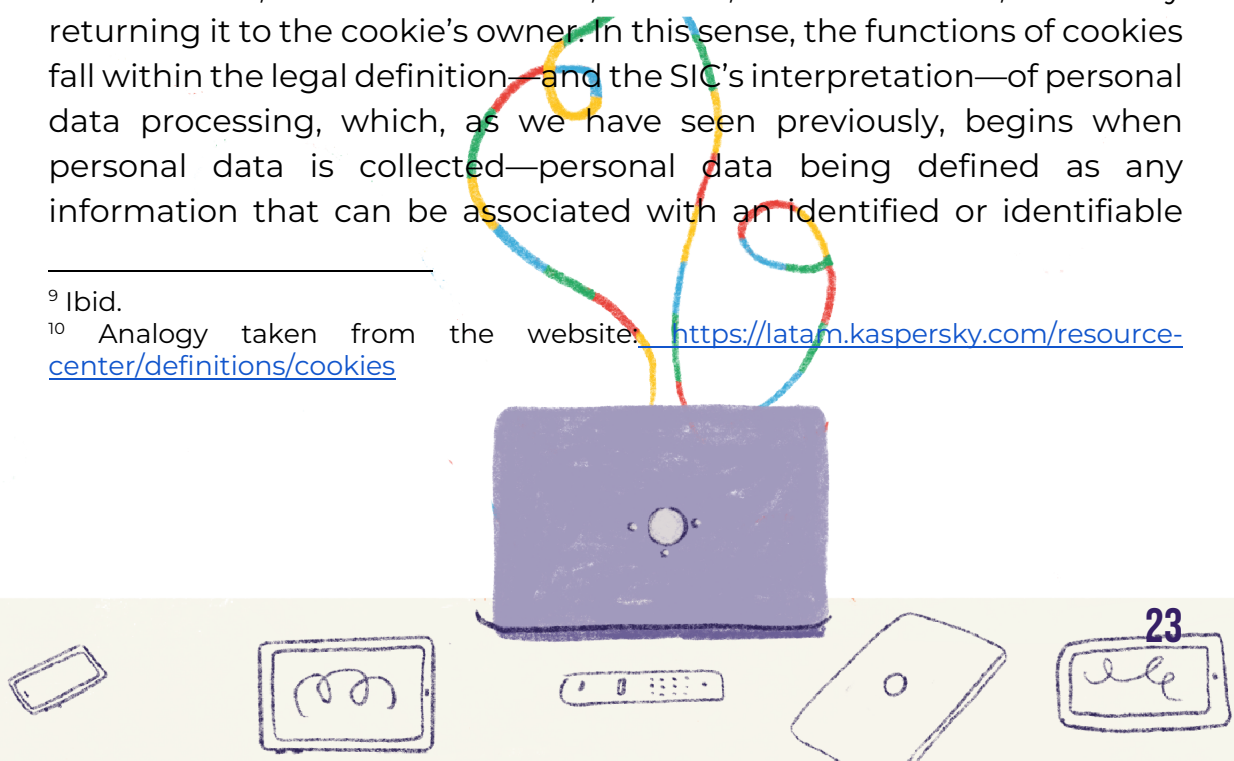
Generally, cookies can only be read by the website being visited—the one that created them. However, there are so-called “third-party cookies,” which result from commercial agreements between tech giants like Google or Meta, allowing these companies to install and create cookies for websites they do not own. In this way, they can, for example, also install their cookies on media websites in order to collect an even broader range of information about users. Like third-party cookies, there are other types of cookies that are named according to their purpose, lifespan, and other characteristics.

Here's an analogy that helps explain how cookies work and what they do: A person goes to a party and, upon arrival, leaves their coat at the coat check; there, the coat check attendant gives them a “ticket” that identifies them as the owner of the coat they've left; the person then goes off to enjoy the party. However, a little while later, they return to the coat check and hand over the “ticket” that identifies them as the owner of the coat¹⁰. In this case, the coat check is the website, the “ticket” is the cookie, and the partygoer is the website user. On the other hand, the cloakroom attendant is the company that creates the cookie to identify the person and collects information about the owner of the coat, since it can identify them through the “ticket.” Upon arriving at the cloakroom, the partygoer is assigned an identification number that will allow the cloakroom to recognize their identity and the activities in which they participated at the party when they return.

Cookies, in fact, use technology that allows them to be installed on a user's device, collect information, store it, and transmit it, ultimately returning it to the cookie's owner. In this sense, the functions of cookies fall within the legal definition—and the SIC's interpretation—of personal data processing, which, as we have seen previously, begins when personal data is collected—personal data being defined as any information that can be associated with an identified or identifiable

⁹ Ibid.

¹⁰ Analogy taken from the website: <https://lata.m.kaspersky.com/resource-center/definitions/cookies>



natural person, in accordance with Article 3 of Law 1581 of 2012—and is intended to obtain information about a natural person.

1.2.2. SDK

Software development kits (SDKs) are “the basic components for creating applications: modular connectors that come preloaded with ready-to-use tools, code, libraries, and tutorials from platforms and/or third parties that form an integral part of the software supply chain”¹¹. Some of these tools are essential for the platforms to function, so they are incorporated into applications and end up being installed on end-users’ devices.

If we wanted to simplify the definition of SDKs, we could draw an analogy with a toolbox that provides everything needed to build a house, from bricks to hammers and screwdrivers¹². In our example, the house represents the applications installed on electronic devices, and the SDKs form the foundation of those applications’ software.

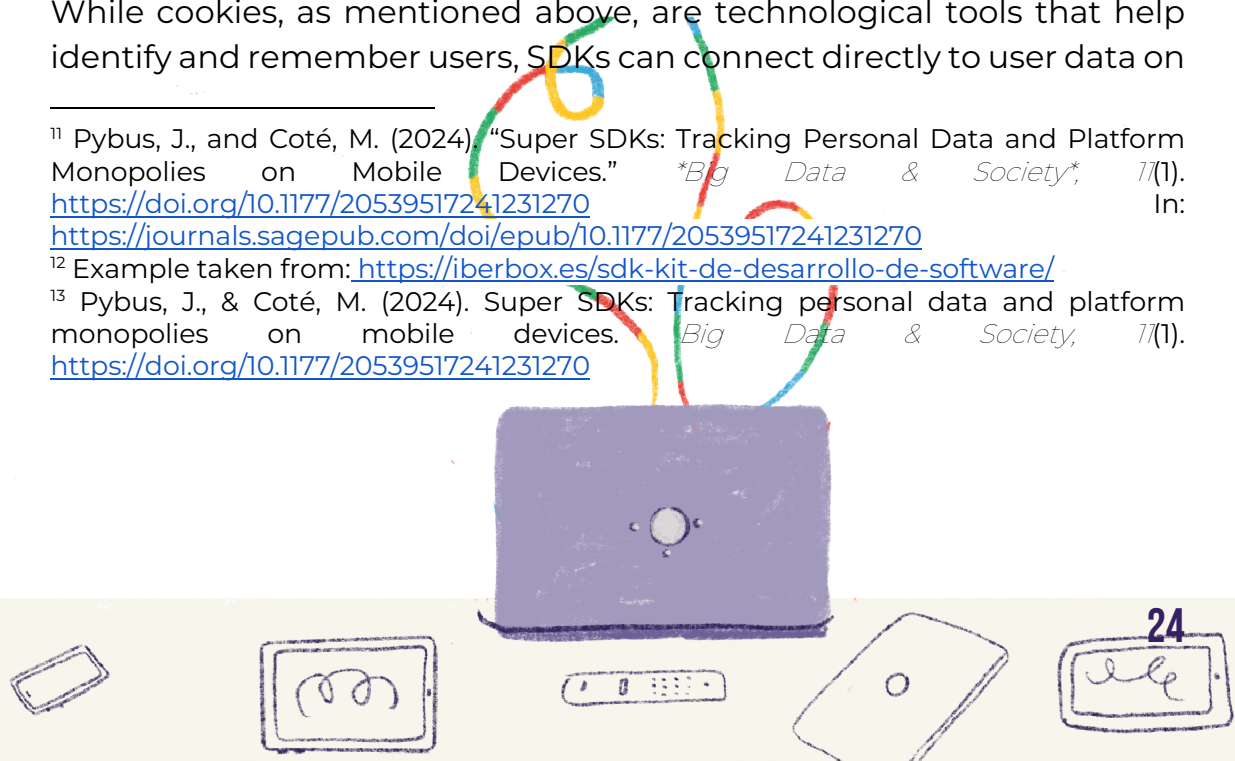
It has been documented that, while SDKs play—in principle—an indispensable role in application development, they have also become tools used for the collection of personal data. In fact, the fact that devices have a closed environment—that is, a controlled, integrated environment limited to the apps that come pre-installed on the phone or that the user downloads—“allows any app to establish a much more intimate relationship with end users”¹³. In this regard, once installed on the device—and depending on their functionality—SDKs can collect data from the device user, such as their location, where they click, or where they navigate within the app.

While cookies, as mentioned above, are technological tools that help identify and remember users, SDKs can connect directly to user data on

¹¹ Pybus, J., and Coté, M. (2024). “Super SDKs: Tracking Personal Data and Platform Monopolies on Mobile Devices.” **Big Data & Society**, 11(1). <https://doi.org/10.1177/20539517241231270>
In: <https://journals.sagepub.com/doi/epub/10.1177/20539517241231270>

¹² Example taken from: <https://iberbox.es/sdk-kit-de-desarrollo-de-software/>

¹³ Pybus, J., & Coté, M. (2024). Super SDKs: Tracking personal data and platform monopolies on mobile devices. *Big Data & Society*, 11(1). <https://doi.org/10.1177/20539517241231270>



mobile devices. In addition, apps also contain third-party SDKs, which means that apps developed by Company X may also have SDKs from Company W integrated into them. Third-party SDKs are used to provide various functionalities, such as “user authentication and data encryption, as well as specialized components like analytics, ad serving, and user interface enhancements”¹⁴ and others.

By 2025, for example, it was found that “most Android apps incorporate multiple third-party SDKs, with an average of approximately 8.6 SDKs per app”¹⁵. This average, combined with the opaque data-processing practices of some SDKs, can jeopardize the rights to privacy or the protection of personal data¹⁶.

It is worth reiterating that this data collection begins when apps are downloaded onto mobile devices. These apps contain SDKs that enable the collection of users’ personal data—sometimes for the app developer and other times for third parties.

1.2.3. PIXELS

Pixels are small, transparent images embedded in web pages or emails¹⁷. They are invisible to the human eye but are highly capable of collecting and tracking personal data, such as IP addresses, operating systems, browsers used, online behavior, and more. Pixels can track how users interact with a website and can be used to monitor consumer behavior and display personalized ads¹⁸.

¹⁴ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G., and Dong, J. S. (2025). Evaluation of privacy compliance in third-party SDKs for Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>

¹⁵ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G., and Dong, J. S. (2025). Evaluation of privacy compliance in third-party SDKs for Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>

¹⁶ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G., and Dong, J. S. (2025). Evaluation of privacy compliance in third-party SDKs for Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>

¹⁷ Newman, L. H. (2022). The Viral Internet Image You've Never Seen. In T. Bosch (Ed.), *You're Not Supposed to Understand This: How 26 Lines of Code Changed the World*. Princeton University Press. <https://www.jstor.org/stable/j.ctv2ks6t89.18>

¹⁸ Federal Trade Commission, Office of Technology. (March 16, 2023). *Lurking Beneath the Surface: The Hidden Impacts of Pixel Tracking*.



Technically, these pixels are small pieces of code that allow for the tracking of users' online activities once they visit a website. Unlike cookies, users are unaware that pixels are being used. In fact, "to mitigate the use of tracking pixels on your own, you typically have to use browser extensions that may disrupt the website's functionality, disable all image requests on a site, or view emails in plain text only"¹⁹. In other words, disabling this tracking technology requires advanced technical knowledge.

According to the U.S. Consumer Protection Agency, pixels can be monetized in various ways: through the sale of targeted advertising, the optimization of the platforms' own targeting systems, and other methods. In 2022, The Markup and STAT—alternative media outlets focused on technology and health, respectively—reviewed 100 U.S. hospital websites. On 33 of them, they found a tracker called the Meta Pixel that "sent a data packet to Facebook every time a person clicked a button to schedule a doctor's appointment." The data is linked to an IP address—an identifier that is like a computer's mailing address and can generally be associated with a specific person or household—which provides Facebook with a detailed record of the appointment request"²⁰.

As part of their research, they also examined websites used to provide telehealth services and found that 13 of the 50 sites contained at least one tracker from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn, or Pinterest²¹. These trackers—in some cases, pixels—collected information about responses related to "self-harm, drug and alcohol

<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>

¹⁹ Newman, L. H. (2022). The Viral Internet Image You've Never Seen. In T. Bosch (Ed.), *You're Not Supposed to Understand This: How 26 Lines of Code Changed the World*. Princeton University Press. <https://www.jstor.org/stable/j.ctv2ks6t89.18>

²⁰ Feathers, T., Fondrie-Teitler, S., Waller, A., & Mattu, S. (June 16, 2022). *Facebook Is Collecting Confidential Medical Information from Hospital Websites*. The Markup. <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

²¹ Feathers, T., Palmer, K., and Fondrie-Teitler, S. (December 13, 2022). "Out of Control": Dozens of telehealth startups sent confidential health information to big tech companies. The Markup. <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>



use, and [...] personal data—including name, email address, and phone number—and sent it to Facebook”²² . As we have seen, these small pieces of code embedded in transparent images in emails or on web pages have the potential to collect data from anyone who opens the email or visits the website, and they are used by various tech giants.

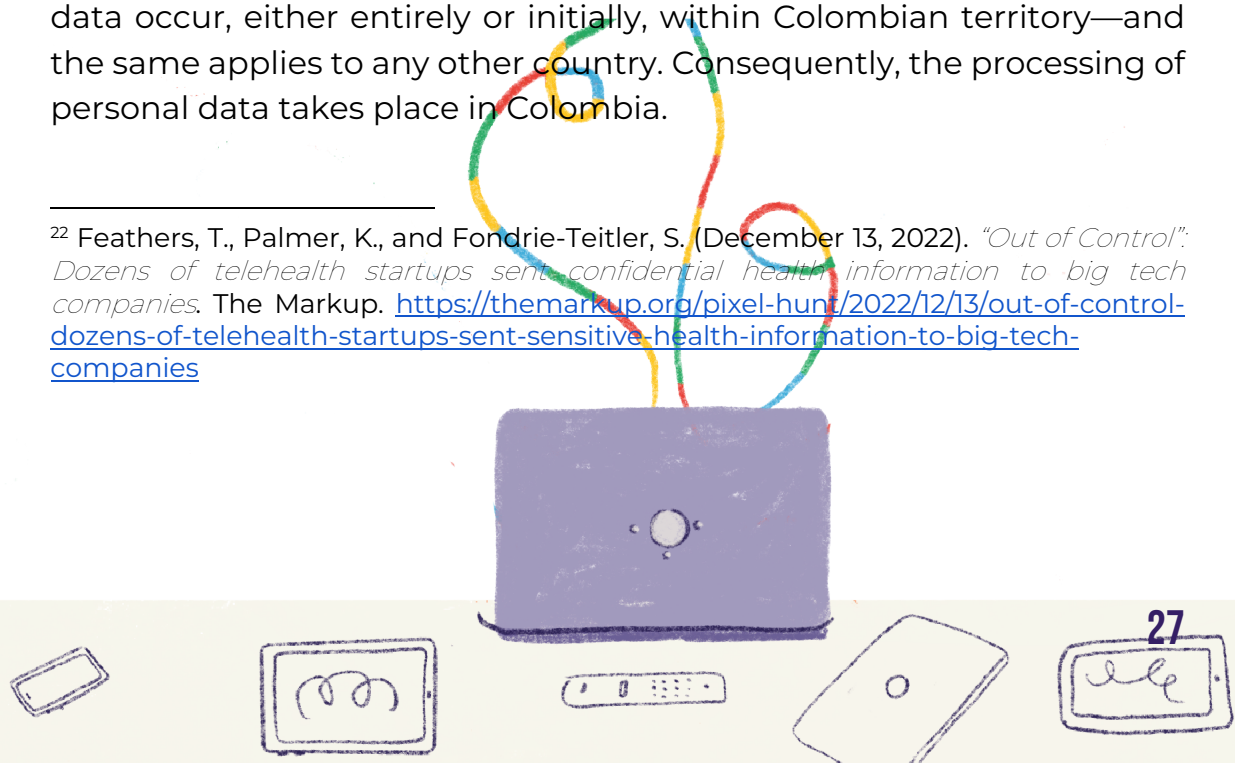
1.3. THE PROCESSING OF PERSONAL DATA THROUGH THESE TECHNOLOGIES TAKES PLACE IN COLOMBIA AND OTHER COUNTRIES IN THE GLOBAL SOUTH

Having explained how local data collection works through cookies, SDKs, and pixels—and knowing that there are many other methods used by tech giants to process personal data—we will now explain why it can be asserted that this processing of personal data takes place in Colombia and is therefore subject to Law 1581 of 2012. We also emphasize that this argument extends to other countries where, without a doubt, the data collection and processing techniques are the same and where the data of their residents is being processed.

Let us recall that cookies are mechanisms that enable the collection of personal data, the storage of information, and the transmission of such information. As explained above, this occurs because cookies are small text files created and sent by websites to users’ devices to obtain and store information about them. This information is retrieved by the website when the same user visits it again.

Persistent cookies—that is, those that last longer and do not expire with each session—are stored on the user’s electronic device. If that device is located in Colombia, the collection, transfer, and storage of personal data occur, either entirely or initially, within Colombian territory—and the same applies to any other country. Consequently, the processing of personal data takes place in Colombia.

²² Feathers, T., Palmer, K., and Fondrie-Teitler, S. (December 13, 2022). “Out of Control”: Dozens of telehealth startups sent confidential health information to big tech companies. The Markup. <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>

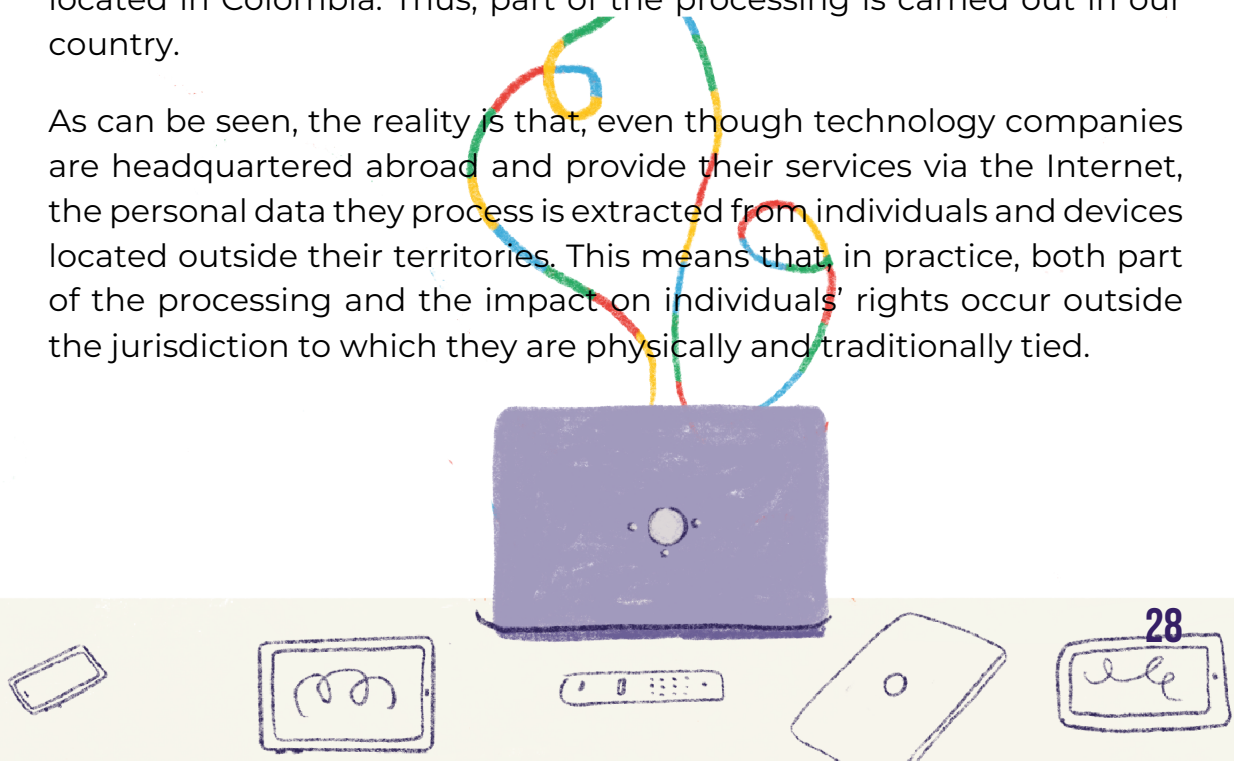


In fact, in this scenario, the data is collected from a user located in Colombia and is then stored in a cookie installed on their device—which is also located in Colombia. Next, a data transmission process begins in Colombia, since when the user returns and visits the same website, the cookie is transferred from the device located in Colombia to the website's server, which intends to read the information. Thus, even if the server receiving the data is located in another country, this data collection initially took place in Colombia, since the device is located within our territory. Consequently, it is in Colombia where the cookie was installed and where the data enabling the user to be identified on future visits was captured.

A similar situation arises in the case of SDKs. As described above, SDKs are basic components necessary for the operation of technology applications. These applications, in turn, are available for download on platforms such as the Google Play Store or the Apple App Store. Once the applications are installed on mobile devices located in Colombian territory, they run their own SDKs and those of third parties, which facilitates the collection of data from the applications' users. This collection takes place in Colombia—or in the country where the user is located—to the extent that the applications and their operational SDKs are installed on mobile devices located within our territory. Therefore, the collection occurs within Colombian territory.

Finally, we would like to emphasize that, although the pixels are not downloaded to the device, they are transparent images that—though invisible to the human eye—are displayed on the screens of users' devices. Once the data collection order takes effect, it may be sent from a server abroad, but the collection itself takes place on the device located in Colombia. Thus, part of the processing is carried out in our country.

As can be seen, the reality is that, even though technology companies are headquartered abroad and provide their services via the Internet, the personal data they process is extracted from individuals and devices located outside their territories. This means that, in practice, both part of the processing and the impact on individuals' rights occur outside the jurisdiction to which they are physically and traditionally tied.



A traditional and anachronistic interpretation of territoriality has led large technology companies to resist complying with the data protection laws of the countries where they process data and from which they extract personal data that they monetize. This has occurred primarily in countries of the Global South, which lack political capital even remotely comparable to that of the European Union, which has successfully enforced its regulations on personal data protection.

In Colombia, for example, the Office for the Protection of Personal Data within the Superintendency of Industry and Commerce (SIC) has made significant efforts to ensure the protection of Colombians' personal data. The SIC has based its jurisdiction and the enforcement of Colombian law precisely on the fact that the processing of personal data takes place in Colombia, and has issued rulings requiring large companies to comply with the legal requirements for such processing.

However, at least three of these large technology companies have filed lawsuits²³ to challenge the SIC's jurisdiction and refuse to comply with Colombian law. Among the arguments put forward by these companies, they emphasize that, in their view, the processing of personal data does not take place on Colombian territory but rather on servers located abroad; that, in the absence of an international, bilateral, or multilateral treaty authorizing the Colombian data protection authority to hear their cases, any measure adopted by the authority is

²³ **Case "Google LTDA,"** Case No.: 25000234100020220044800, Subject: Annulment and reinstatement with provisional suspension of Resolutions 70315, dated November 4, 2020, and 38869, dated June 24, 2021; Filed on April 21, 2022; Presiding Judge: LUIS NORBERTO CERMEÑO; Plaintiff: GOOGLE COLOMBIA LTDA; Defendant: SUPERINTENDENCY OF INDUSTRY AND COMMERCE; **Google LLC Case,** Case No.: 25000234100020220044400, Subject: Annulment and restoration of rights with provisional suspension of Resolutions No. 53593, dated September 3, 2020, No. 14010, dated March 16, 2021, and No. 60478, dated September 21, 2021, Filed on April 20, 2022, Presiding Judge: ANA MARGOTH CHAMORRO BENAVIDES, Plaintiff: GOOGLE LLC, Defendant: SUPERINTENDENCY OF INDUSTRY AND COMMERCE; **WhatsApp Case,** Plaintiff: WhatsApp LLC, Defendant: SIC, Case No.: 25000-23-41-000-2022-01520-00, Subject: Annulment and restoration of rights regarding Resolutions 4554 of 2022, 29826 of 2021, and 15342 of 2022; Judge: Ana Margoth Chamorro Benavides; Date of complaint: 12/06/2022; **TikTok Case,** Plaintiff: Bytedance LTD, Defendant: SIC, Case No.: 25000234100020220106400, Subject: Annulment and restoration of rights — Decisions No. 62132, dated October 5, 2020, No. 14015, dated March 16, 2021; and No. 75009, dated November 22, 2021, issued by the SIC.



invalid; and that they have their registered offices in other countries and do not maintain offices within Colombian territory. However, in most cases, these companies are majority shareholders and exercise control over companies incorporated under Colombian law, even though they maintain that they are independent legal entities.

Ultimately, this highlights the lack of protection faced by millions of people who use digital services daily in countries other than those where the large companies providing them are headquartered. These individuals are left defenseless against the immense economic and political power of large technology companies, which end up extracting their data and turning it into a significant economic asset. This data is then used to personalize content and, at times, to manipulate people's minds, influencing not only consumer decisions but also political preferences and other areas. In the following sections, we delve deeper into some of these dimensions and how these risks have materialized in various countries across the region.

1.4. MAJOR PLATFORMS HAVE BEEN HELD ACCOUNTABLE IN OTHER JURISDICTIONS

The processing of personal data across different territories poses a challenge when it comes to evaluating it and ensuring the legal protection of data subjects. In this context, various courts around the world have recognized that companies headquartered abroad cannot evade the application of local data protection laws by formally claiming that they do not have a registered office in a specific country. The following are some examples:

1.4.1. THE GOOGLE SPAIN V. AEPD CASE (2014)

In 2014, the Court of Justice of the European Union (CJEU) ruled on the aforementioned case **of Google Spain v. the Spanish Data Protection Agency (C-131/12)**²⁴. The case arose from a request by a Spanish citizen for Google to remove from its search results a link that damaged his

²⁴ CJEU. Google Spain v. AEPD (C-131/12, 2014). Available at: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131>



reputation. Google argued that European data protection regulations did not apply to it, since its headquarters were located in the United States and data processing took place outside European territory.

The Court rejected this argument and concluded that Google was subject to European law, as there was a direct link between the activities of the U.S. parent company and those of its subsidiary in Spain. In the Court's view,

“Google Inc. manages Google Search from a technical and administrative standpoint, and it has not been demonstrated that Google Spain carries out any activities in Spain directly related to the indexing or storage of information or data contained on third-party websites. However, **the promotion and sale of advertising space—for which Google Spain is responsible in Spain—constitutes the essential part of the Google group's commercial activity and can be considered closely linked to Google Search.**”²⁵ (bold added).

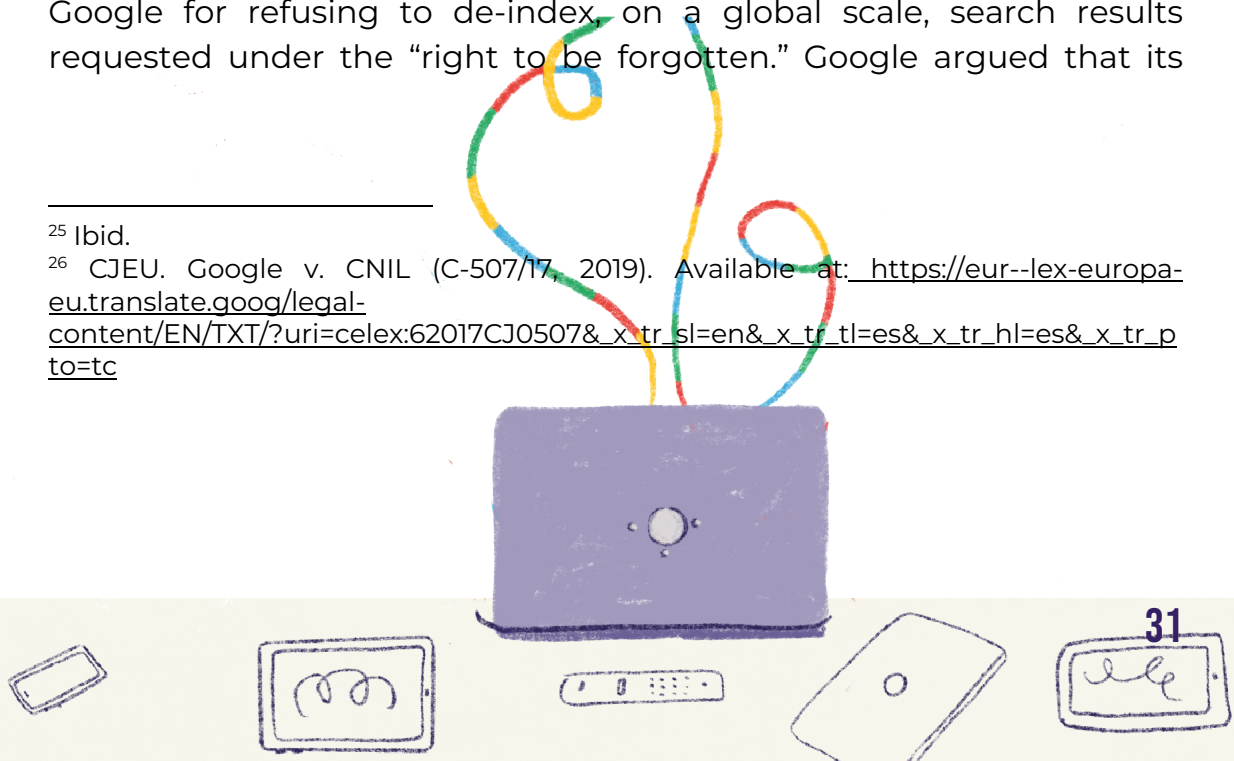
Thus, the CJEU interpreted the concept of “establishment” broadly and established a standard for the functional application of the law: when a company operates in a territory through subsidiaries that enable or make its economic activity profitable, it is required to comply with that country's data protection regulations.

1.4.2. THE GOOGLE V. CNIL CASE (2019)

Another significant precedent was the **Google LLC v. CNIL case**, decided in 2019 by the CJEU²⁶ and subsequently by the French Council of State. The French data protection authority (CNIL) imposed a fine on Google for refusing to de-index, on a global scale, search results requested under the “right to be forgotten.” Google argued that its

²⁵ Ibid.

²⁶ CJEU. Google v. CNIL (C-507/17, 2019). Available at: https://eur-lex.europa.eu.translate.google/legal-content/EN/TXT/?uri=celex:62017CJ0507&x_tr_sl=en&x_tr_tl=es&x_tr_hl=es&x_tr_p to=tc



obligation should be limited to the European domains of its search engine and should not extend to the rest of the world.

The Court of Justice of the European Union acknowledged that the protection of the “right to be forgotten” must be balanced against the freedom of information, but made it clear that national authorities may require the extraterritorial application of the rules when necessary to ensure the effectiveness of individuals’ rights. This ruling echoes the reasoning in the Spanish case, in that

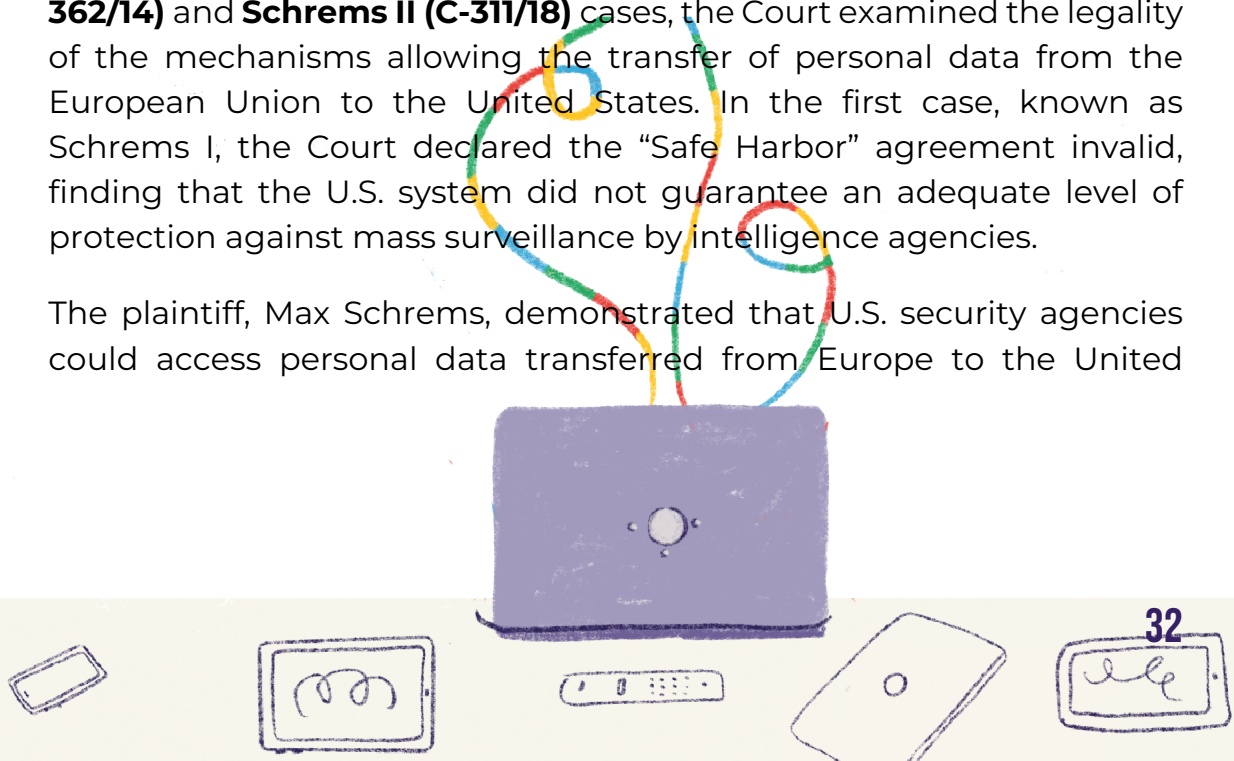
“[T]he Google establishment on French territory **carries out, among other things, commercial and advertising activities that are inextricably linked to the processing of personal data for the operation of the search engine** in question; and, second, that said search engine—given, among other things, the existence of gateways between its various national versions—must be considered to **carry out a single processing of personal data**. The referring court considers that, in these circumstances, such processing is carried out within the framework of Google’s establishment in France” (emphasis added)

In its final ruling, the French Council of State upheld the penalty imposed by the CNIL and emphasized that global companies must ensure consistent compliance with data protection decisions across all territorial versions of their services.

1.4.3. THE SCHREMS I (2015) AND SCHREMS II (2020) CASES

Following the Google Spain case, the CJEU expanded its case law on the cross-border dimension of “habeas data.” In the **Schrems I (C-362/14)** and **Schrems II (C-311/18)** cases, the Court examined the legality of the mechanisms allowing the transfer of personal data from the European Union to the United States. In the first case, known as Schrems I, the Court declared the “Safe Harbor” agreement invalid, finding that the U.S. system did not guarantee an adequate level of protection against mass surveillance by intelligence agencies.

The plaintiff, Max Schrems, demonstrated that U.S. security agencies could access personal data transferred from Europe to the United



States without effective judicial oversight, which violated the principles of proportionality and necessity in data processing. The CJEU concluded that European companies—or those operating in Europe—could not shift their responsibilities to the authorities of another country and that protection must be guaranteed at all times, regardless of where the data was stored.

In **the Schrems II case**, the Court reached an even more forceful conclusion: it invalidated the “Privacy Shield” mechanism—the successor to “Safe Harbor”—reiterating that the protection of personal data is a fundamental right that cannot be undermined by trade agreements or self-regulatory mechanisms. In that ruling, the CJEU held that companies transferring data outside the European Union must ensure that individuals enjoy a level of protection substantially equivalent to that provided by EU law.

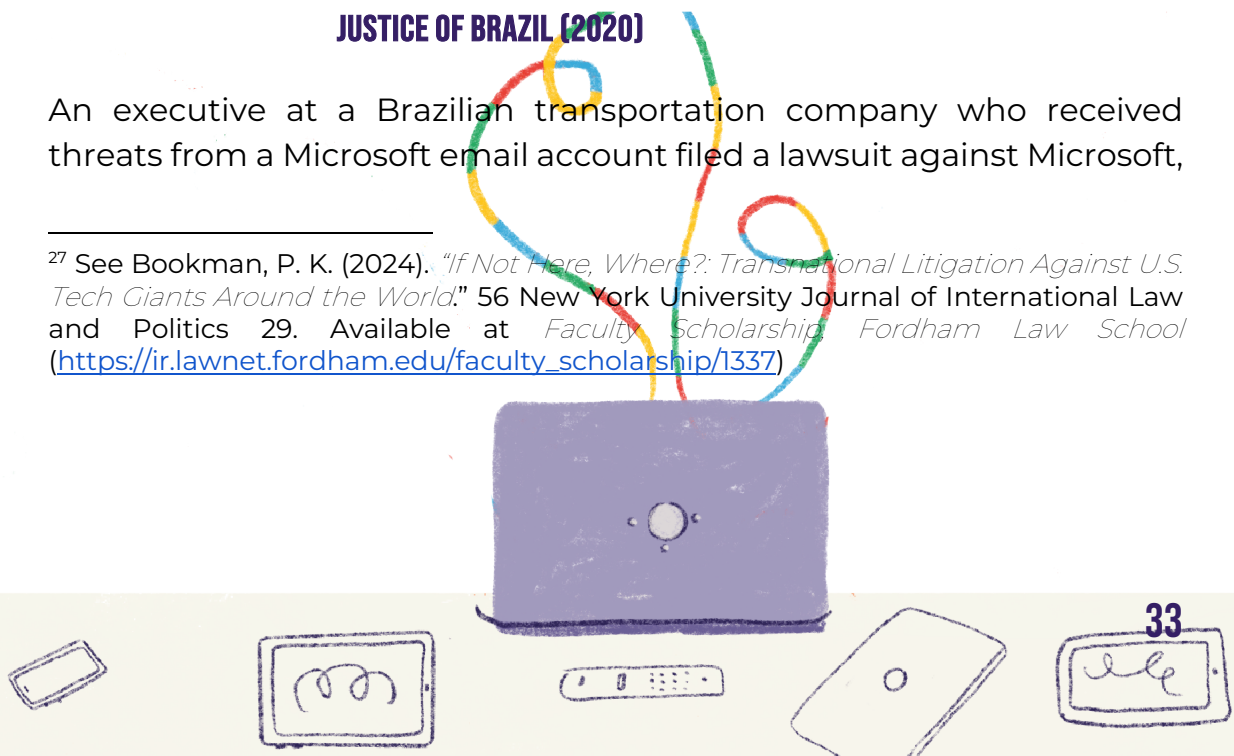
1.4.4. THE TWITTER CASE IN CANADA: GIUSTRA V. TWITTER, INC. (2021)

This case was brought before the courts of British Columbia (Canada) after Mr. Giustra filed a lawsuit over tweets that, in his view, damaged his reputation. Twitter, the defendant in the proceedings, moved to have the case dismissed on the grounds of lack of jurisdiction or “forum non conveniens.” In Twitter’s view, California was the appropriate forum, since it was a U.S. company, the posts had been published primarily in the U.S., and they dealt with political issues in that country. However, both at the trial court level and on appeal, the Canadian courts affirmed their jurisdiction, arguing that the tweets had been posted in British Columbia and had caused harm to a resident of British Columbia²⁷.

1.4.5. THE CASE AGAINST MICROSOFT DECIDED BY THE SUPERIOR COURT OF JUSTICE OF BRAZIL (2020)

An executive at a Brazilian transportation company who received threats from a Microsoft email account filed a lawsuit against Microsoft,

²⁷ See Bookman, P. K. (2024). “If Not Here, Where?: Transnational Litigation Against U.S. Tech Giants Around the World.” 56 New York University Journal of International Law and Politics 29. Available at *Faculty Scholarship Fordham Law School* (https://ir.lawnet.fordham.edu/faculty_scholarship/1337)



requesting that the company provide access logs (IP address, date, and time) that would allow the author of the threats to be identified. The trial court granted a preliminary injunction and set a daily fine of R\$ 10,000 for noncompliance; when the company refused to hand over the data, the fine was provisionally enforced until it reached R\$ 310,000. Microsoft, in its defense, argued that the Brazilian courts lacked jurisdiction because the threats were written in English, the email account had been accessed from abroad, the internet service provider was also located outside Brazil, and that complying with the order would violate U.S. law, where the access allegedly took place. However, Brazil's Superior Court of Justice unanimously rejected this argument, emphasizing that it is sufficient for at least one device (in this case, that of the threatened user) involved in the processing of personal data to be located within national territory for national law to apply, regardless of whether the company is foreign:

"It is a misconception to imagine that any application hosted outside Brazil cannot be subject to national jurisdiction or that Brazilian laws do not apply to its activities. Brazilian law applies whenever any operation involving the collection, storage, retention, and processing of records, personal data, or communications by internet service providers and internet applications **occurs within national territory, even if only one of the devices involved in the communication is in Brazil and even if the activities are carried out by a company headquartered abroad.**" (own translation, summary, points 5 and 6)."

"The appellant, on its own, is a subsidiary company dedicated exclusively to operations in Brazil, but **it belongs to an economic group** that is recognized worldwide." (own translation, para. XXXI by Rapporteur Adigri)

1.4.6. THE CASE OF P.A.E. V. FACEBOOK ARGENTINA S.R.L. (EX PARTE INJUNCTION OF 2019)

In this case, an individual filed a self-executing injunction against Facebook Argentina S.R.L. requesting the removal of posts containing



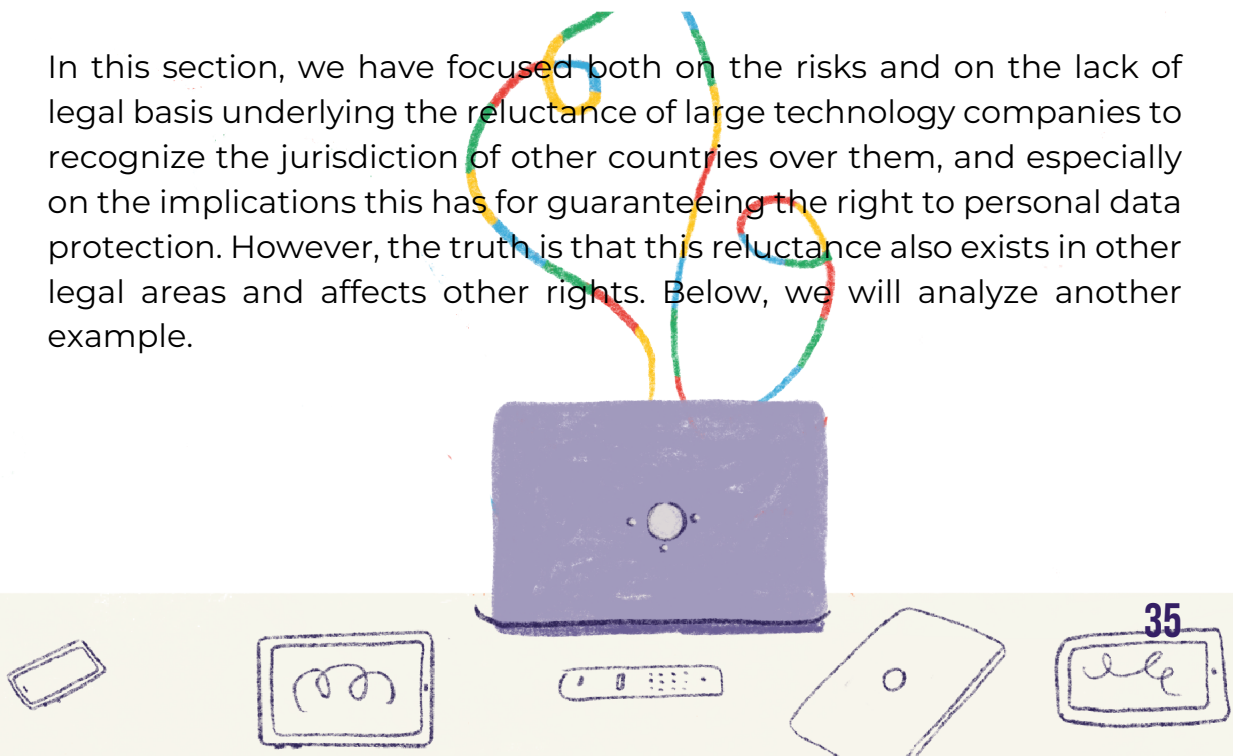
the names and images of his children. The trial judge initially granted the injunction. However, Facebook Argentina appealed that decision, arguing lack of standing to be sued, since it is not the entity that operates the “facebook.com” website. The Superior Court upheld the trial judge’s ruling and noted that the defense of lack of standing was unfounded, given that the subsidiary is subject to Argentine law. The ruling emphasizes that, regardless of the corporate structure the company adopts, it is represented in the country; and that, furthermore, incorporation abroad does not mean that the country’s laws do not apply to it when acts and contracts are entered into within the country:

“A company incorporated abroad is governed, in terms of its existence and form, by the laws of the place of incorporation; however, this **does not preclude the application of Argentine laws to acts and contracts entered into in our** country, since its presence here implies full submission to Argentine jurisdiction and laws, even though its legal capacity is governed by the law of its domicile. Nor can we overlook the fact that social media, as well as other forms of electronic communication and data processing via the Internet, have created a complex framework of jurisdictional competences and responsibilities that require adequate and specific legislation. However, **this situation does not prevent judges from ruling on a specific case.** (...)”

Facebook Argentina S.R.L. cannot evade court orders by claiming it lacks the authority to do so; therefore, the company must acknowledge and comply with the court rulings served at the address it has established in the country.”

1.5. THE CASE OF TAXATION

In this section, we have focused both on the risks and on the lack of legal basis underlying the reluctance of large technology companies to recognize the jurisdiction of other countries over them, and especially on the implications this has for guaranteeing the right to personal data protection. However, the truth is that this reluctance also exists in other legal areas and affects other rights. Below, we will analyze another example.

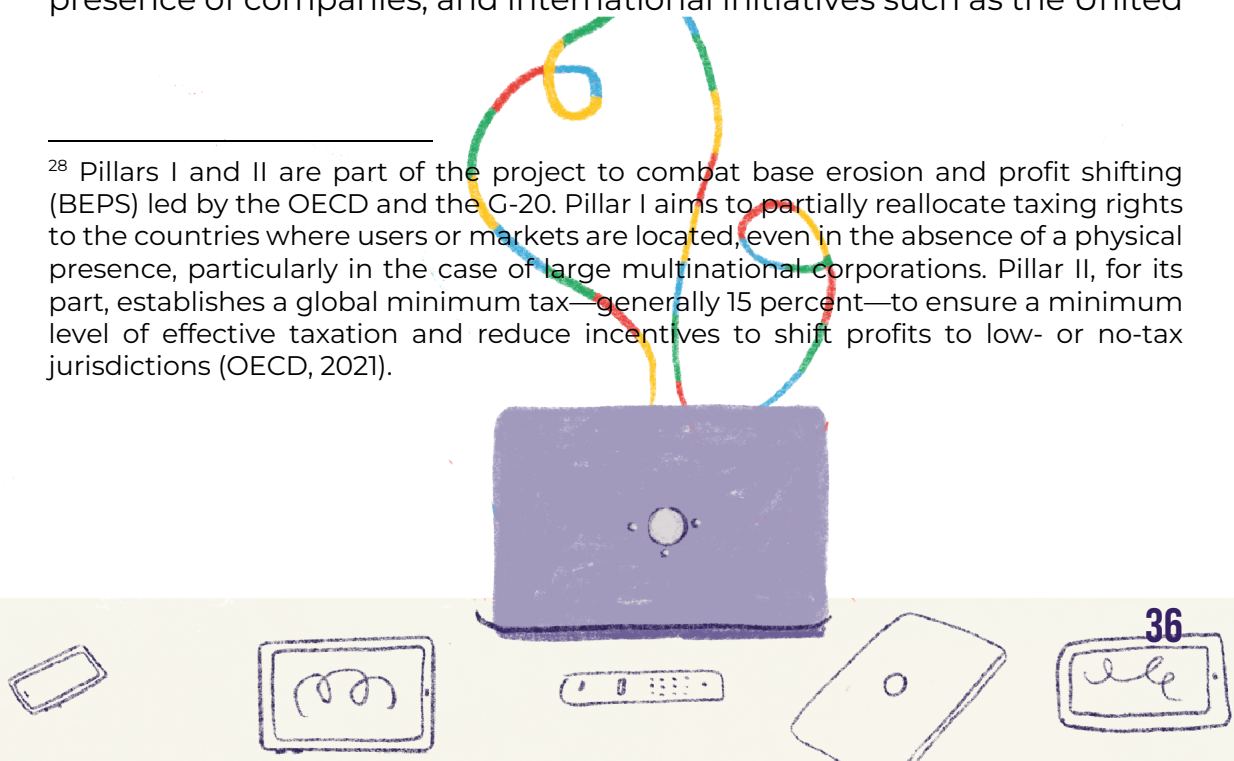


The growing digitization of the economy has highlighted the limitations of the traditional international tax system, which was designed for companies operating through a physical presence in a specific territory. Today, large platforms and digital service providers can generate significant revenue from users and consumers located in countries such as Colombia without needing to establish a physical presence there, which reduces these states' ability to tax the revenue generated in their markets. This phenomenon has been identified by the OECD's BEPS project²⁸ as one of the main challenges in international taxation: while major economies—where the headquarters of digital companies are located—capture a larger share of tax revenue, the countries where users and consumers are located receive a much smaller share of those resources.

This contributes to worsening global inequalities, as it reduces the ability of low-income countries to finance public policies and guarantee fundamental rights to their populations. The revenue that governments can collect constitutes the main source of funding to guarantee rights such as health care, education, social protection, and access to justice. When international rules prevent the countries where consumption and economic value are generated from adequately taxing revenue derived from digital services, their fiscal capacity is diminished, limiting their ability to invest in social sectors.

In this regard, it is essential to seek to strengthen the taxation of cross-border digital services so that the countries where consumption and economic value are generated can participate more equitably in the collection of tax revenue. To this end, mechanisms must be promoted that allow for the taxation of these activities beyond the physical presence of companies, and international initiatives such as the United

²⁸ Pillars I and II are part of the project to combat base erosion and profit shifting (BEPS) led by the OECD and the G-20. Pillar I aims to partially reallocate taxing rights to the countries where users or markets are located, even in the absence of a physical presence, particularly in the case of large multinational corporations. Pillar II, for its part, establishes a global minimum tax—generally 15 percent—to ensure a minimum level of effective taxation and reduce incentives to shift profits to low- or no-tax jurisdictions (OECD, 2021).



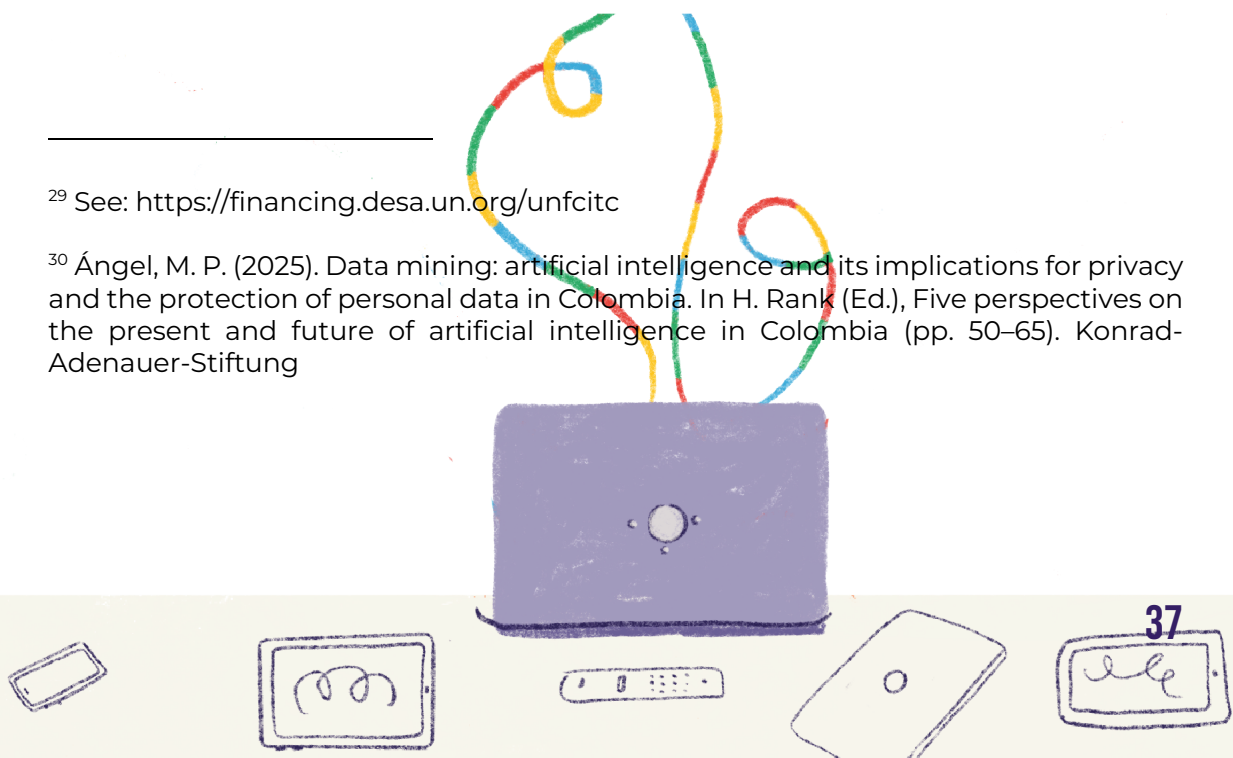
Nations Model Convention on International Tax Cooperation²⁹ —aimed at a more equitable distribution of taxing rights in the digital economy—must be supported.

1.6. CONCLUSION: TECHNOLOGY COMPANIES ARE VIOLATING THE RIGHTS TO PERSONAL DATA PROTECTION AND OTHER FUNDAMENTAL RIGHTS OF MILLIONS OF PEOPLE LIVING IN COUNTRIES SUCH AS COLOMBIA BY REFUSING TO COMPLY WITH NATIONAL REGULATIONS AND TO RECOGNIZE THE JURISDICTION OF THEIR AUTHORITIES.

The failure to recognize the jurisdiction and authority of governments such as Colombia's, as well as the reluctance of large digital technology companies to comply with the laws of countries where they are not headquartered, is leading to serious human rights violations. In this section, we focus primarily on the right to habeas data, as we believe that personal data is the driving force behind the business model of large technology companies and constitutes their most important asset. We also focus on this specific right because its violation threatens "other rights that may be affected due to the massive availability of personal data in the hands of third parties and the greater computational power this grants to those who process it"³⁰. In fact, as will be discussed later, certain population groups are particularly vulnerable to the use of their data, and essential values such as democracy are at risk due to the manipulative use of personal data. Similarly, rights such as physical and mental health are affected by addictive design, profiling, and the influence on consumer habits.

²⁹ See: <https://financing.desa.un.org/unfcitc>

³⁰ Ángel, M. P. (2025). Data mining: artificial intelligence and its implications for privacy and the protection of personal data in Colombia. In H. Rank (Ed.), Five perspectives on the present and future of artificial intelligence in Colombia (pp. 50–65). Konrad-Adenauer-Stiftung



To the extent that current interactions take place primarily—though not exclusively—in cyberspace³¹ and via the Internet, it is essential to strengthen the authority and jurisdiction of local authorities to protect the rights of their citizens. This is the view of the Constitutional Court of Colombia, which has insisted that “the State cannot relinquish its jurisdiction over the Internet”³² ; therefore, in this case, the principle of territoriality is used “to determine whether the dispute has a relevant connection to the country, such as the provision of services to users in Colombia or the processing of personal data within the national territory”³³ . The Court has also noted that, “when a threat or violation of fundamental rights occurs in cyberspace, the judge hearing the tutela petition will have jurisdiction to rule on whether such a threat or violation has relevant effects in Colombia”³⁴ .

2. WEAKENING OF REGULATIONS PROTECTING PERSONAL DATA COLLECTED BY PLATFORMS AND ITS TRANSFER TO THE UNITED STATES UNDER BILATERAL AGREEMENTS

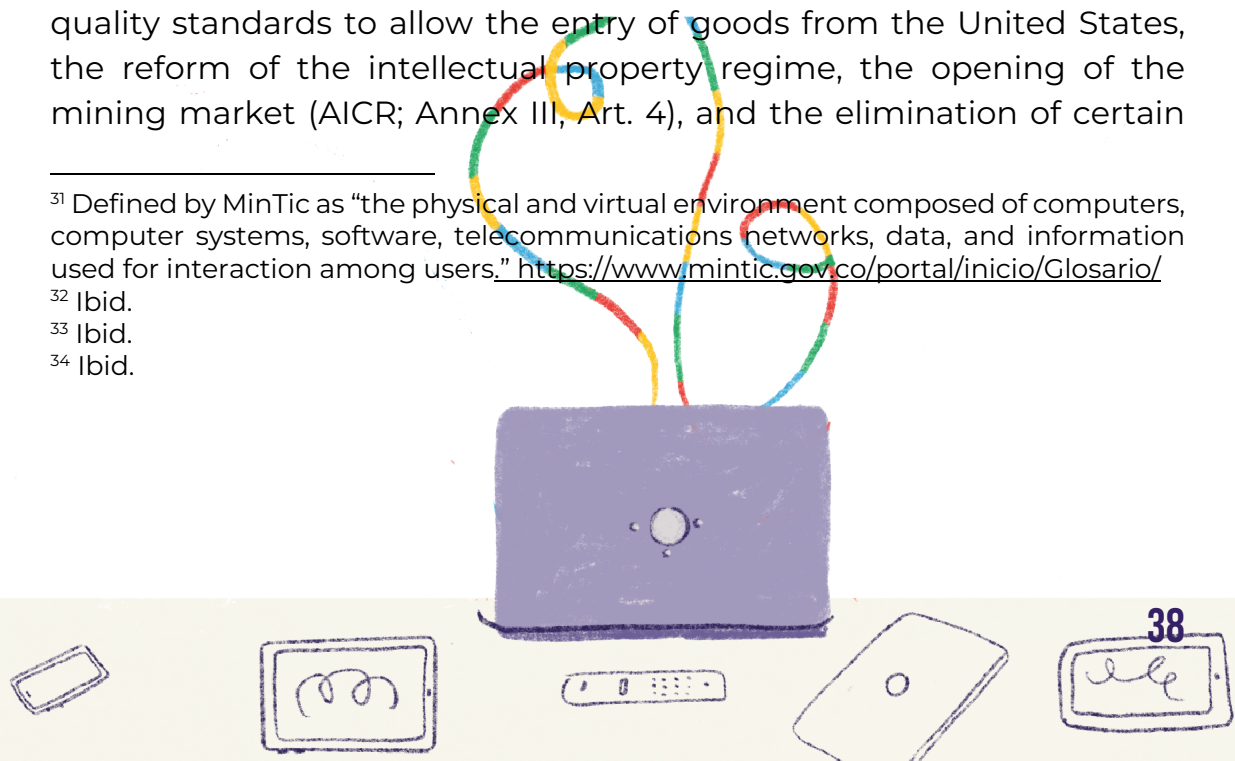
The Agreement between the United States of America and the Argentine Republic on Investment and Reciprocal Trade (“AICR”), signed in February 2026, liberalizes trade between the two countries through the Argentine Republic’s elimination of tariff and non-tariff barriers on U.S. products, the reduction of subsidies and trade privileges for Argentine state-owned enterprises, the harmonization of national quality standards to allow the entry of goods from the United States, the reform of the intellectual property regime, the opening of the mining market (AICR; Annex III, Art. 4), and the elimination of certain

³¹ Defined by MinTic as “the physical and virtual environment composed of computers, computer systems, software, telecommunications networks, data, and information used for interaction among users.” <https://www.mintic.gov.co/portal/inicio/Glosario/>

³² Ibid.

³³ Ibid.

³⁴ Ibid.

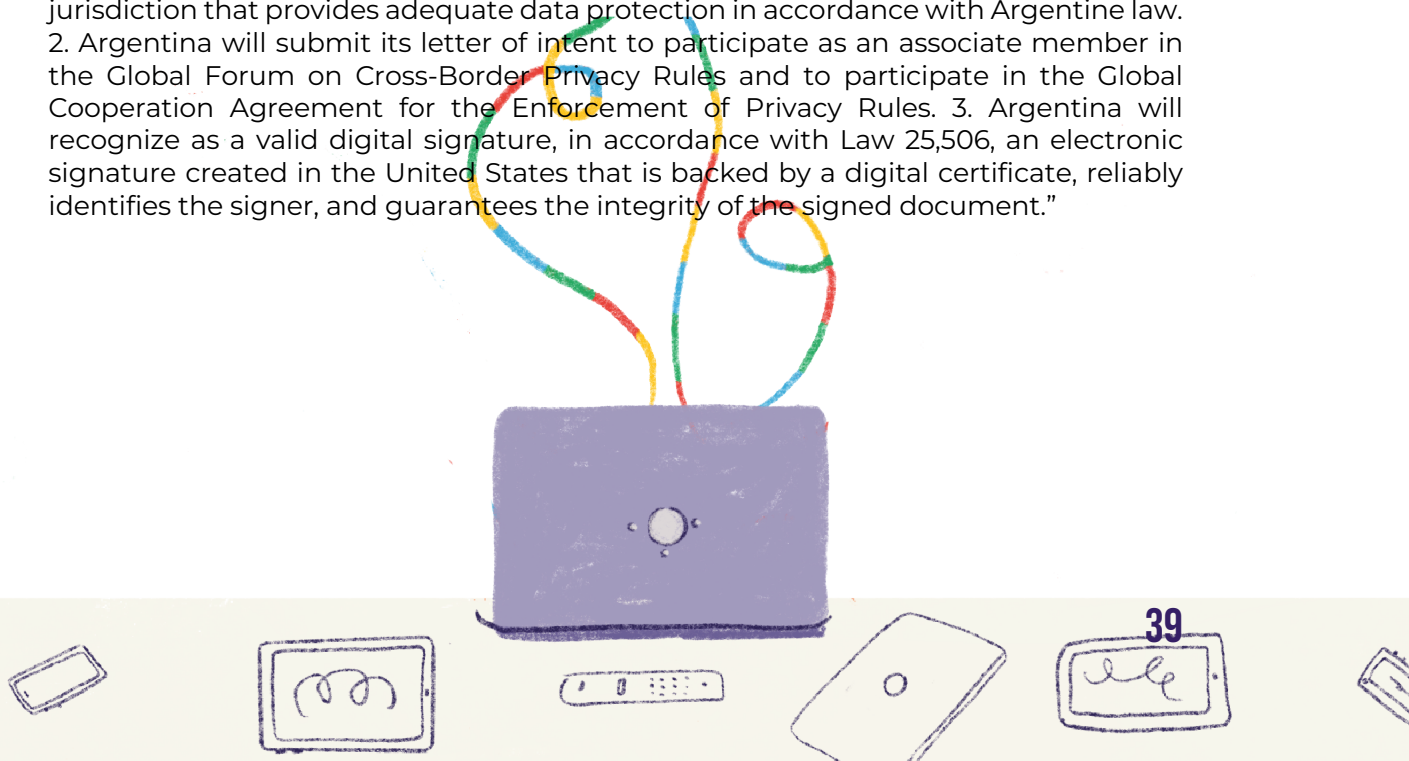


protections for personal data (AICR; Annex III, Art. 2). The AICR will enter into force sixty days after the date on which both States certify compliance with their respective domestic legal requirements (AICR; 6.7). In the Argentine Republic, this means that the treaty must be approved by Congress (National Constitution [CN], Art. 75, Section 22), since the instrument contains obligations that fall within the jurisdiction of the legislative branch and exceed the scope of the executive branch's authority.

Article 2 of Annex III of the AICR, which details the commitments undertaken by Argentina under the treaty, contains a series of significant amendments to the national legal framework regarding personal data.

The AICR aims to “provide legal certainty” for the export to the United States of personal data collected in the Argentine Republic. In this regard, the AICR establishes that, for the purposes of transferring personal data to the United States, Argentina shall consider that the United States guarantees “adequate” legal protection for such data³⁵. Furthermore, the AICR provides for the Argentine Republic's participation in multilateral forums through which the cross-border flow of data and international cooperation among data protection authorities are promoted. Finally, the AICR establishes that documents signed electronically in the United States must be considered equivalent to digitally signed documents, producing the same legal effects as a digital signature and meeting the requirements of integrity

³⁵ AICR, Annex III, Art. 2 (“Digital Trade and Technology. 1. Argentina shall ensure legal certainty regarding the possibility of transferring personal data from its territory to the United States, among other things, by recognizing the United States as a country or jurisdiction that provides adequate data protection in accordance with Argentine law. 2. Argentina will submit its letter of intent to participate as an associate member in the Global Forum on Cross-Border Privacy Rules and to participate in the Global Cooperation Agreement for the Enforcement of Privacy Rules. 3. Argentina will recognize as a valid digital signature, in accordance with Law 25,506, an electronic signature created in the United States that is backed by a digital certificate, reliably identifies the signer, and guarantees the integrity of the signed document.”)



and authenticity established in national legislation (Law 25,506; Articles 5, 7, 8, 9, and 11).

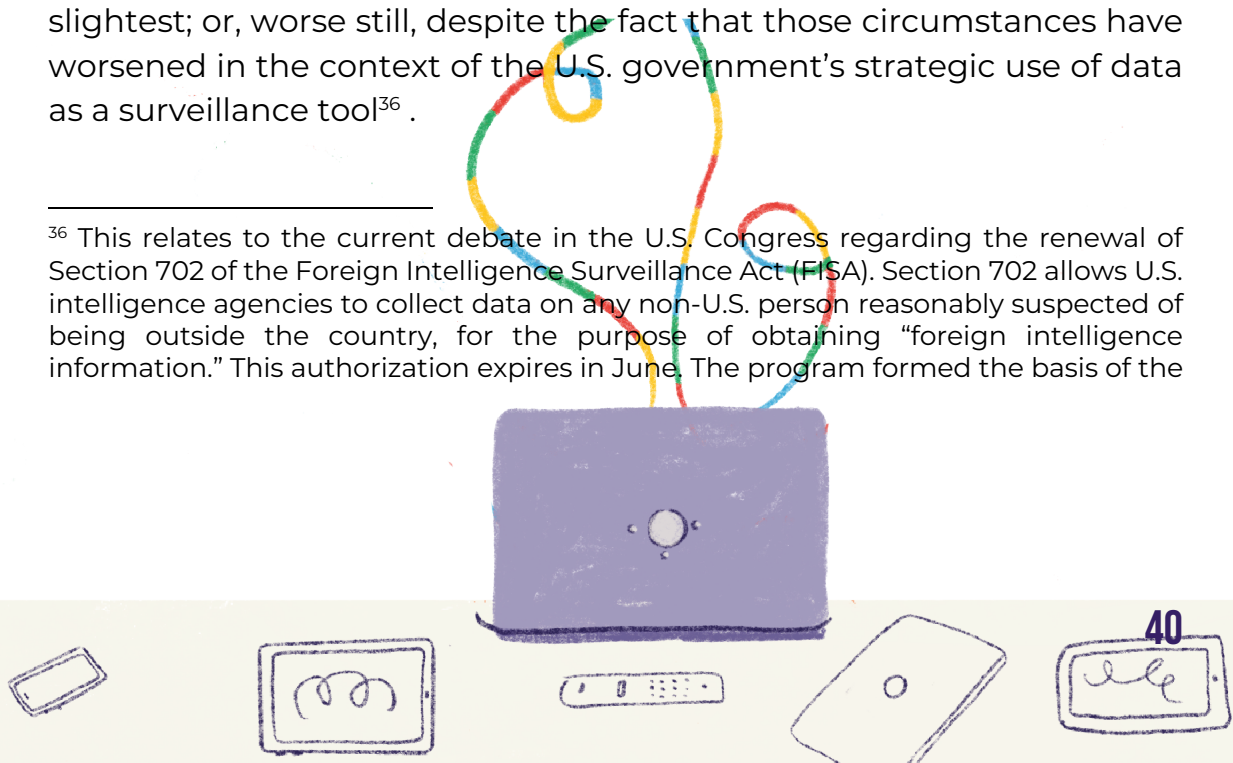
Article 12 of Law 25,326 prohibits the transfer of personal data of any kind to “countries or international or supranational organizations that do not offer adequate levels of protection.” The Agency for Access to Public Information (AAIP) determines, either on its own initiative or at the request of a party, which countries or organizations offer adequate legal protection (Decree 1558/2001; Annex I, 12).

The United States has never been and is not currently included on the list of countries that, according to the AAIP, provide adequate legal protection for personal data. The factors that, in the opinion of the Argentine regulatory authority, raise concerns are:

- Unlike the Argentine Republic, the United States lacks uniform federal regulations on the processing of personal data and an effective supervisory authority.
- Consequently, “self-regulatory” standards are neither enforceable nor uniform across the fifty states of the Union.

The AICR would constitute an exception to the prohibition on transfers of personal data, either as an “international treaty to which Argentina is a party” (as established in Article 12 of Law 25,326) or because the AAIP issues—whether by instruction from the president or through voluntary compliance with the agreement—a resolution declaring that the United States is an adequate jurisdiction. This implies authorizing international data transfers to a country that, until now, was not considered an “adequate jurisdiction” by the Argentine government, without the circumstances in that country having changed in the slightest; or, worse still, despite the fact that those circumstances have worsened in the context of the U.S. government’s strategic use of data as a surveillance tool³⁶.

³⁶ This relates to the current debate in the U.S. Congress regarding the renewal of Section 702 of the Foreign Intelligence Surveillance Act (FISA). Section 702 allows U.S. intelligence agencies to collect data on any non-U.S. person reasonably suspected of being outside the country, for the purpose of obtaining “foreign intelligence information.” This authorization expires in June. The program formed the basis of the



Under the AICR, the sale of personal data to U.S. data controllers or processors—including large technology companies headquartered in that country—will no longer be subject to data protection law or the AAIP, nor will compliance with the model data protection clauses or the requirement for prior administrative authorization be required if they contain different provisions. Simply because their data has been sold to the United States, data subjects will no longer enjoy the protections offered by Argentine law and may be deprived of the protection of Argentine courts.

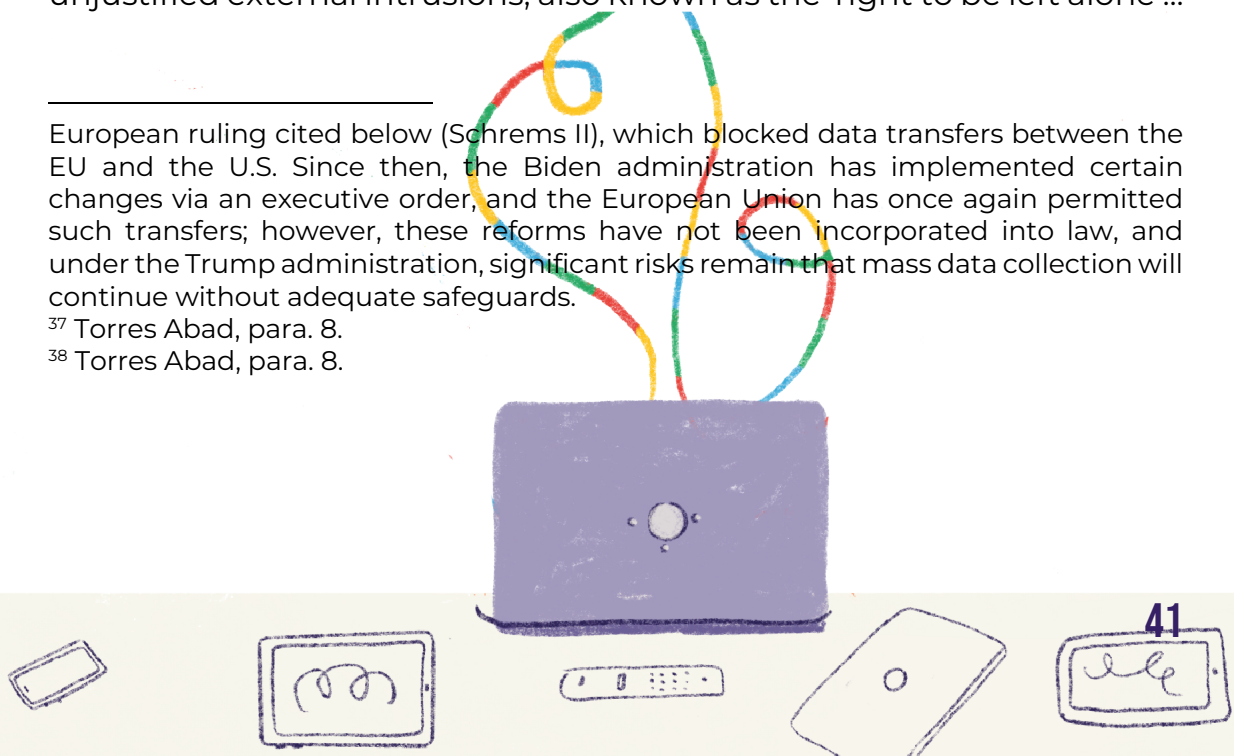
In a recent ruling on the “Torres Abad” case, the Supreme Court of Justice of the Nation interpreted the scope of Articles 19 and 43 of the National Constitution in a manner that conflicts with the provisions of the AICR. In that case, the Court declared the transfer of personal data without the specific consent of the data subjects to be unconstitutional in instances where the personal data protection law authorized such transfers “in the performance of state functions” or pursuant to a legal mandate relating to those authorities, or through agreements entered into among them within the scope of their respective jurisdictions.

The Court held that Articles 19 and 43(3) of the National Constitution enshrine the right to informational self-determination³⁷ —already recognized by the Inter-American Court of Human Rights in the CAJAR case—and the right “to be left alone.” Regarding the former, the Court affirmed that “every person has the right to control the data concerning them, to decide with whom and to what extent they wish to share it, and, where appropriate, to control the use that third parties make of it.”³⁸ Furthermore, the Supreme Court recognized “the right of every person to enjoy solitude and tranquility, without being disturbed by unjustified external intrusions, also known as the ‘right to be left alone’...

European ruling cited below (Schrems II), which blocked data transfers between the EU and the U.S. Since then, the Biden administration has implemented certain changes via an executive order, and the European Union has once again permitted such transfers; however, these reforms have not been incorporated into law, and under the Trump administration, significant risks remain that mass data collection will continue without adequate safeguards.

³⁷ Torres Abad, para. 8.

³⁸ Torres Abad, para. 8.



or the ‘right to be left in peace.’”³⁹ It also noted that the legal exceptions relating to the “performance of state functions” or equivalent were so broad that, on their own, they did not satisfy the requirements of legitimate purpose or proportionality.

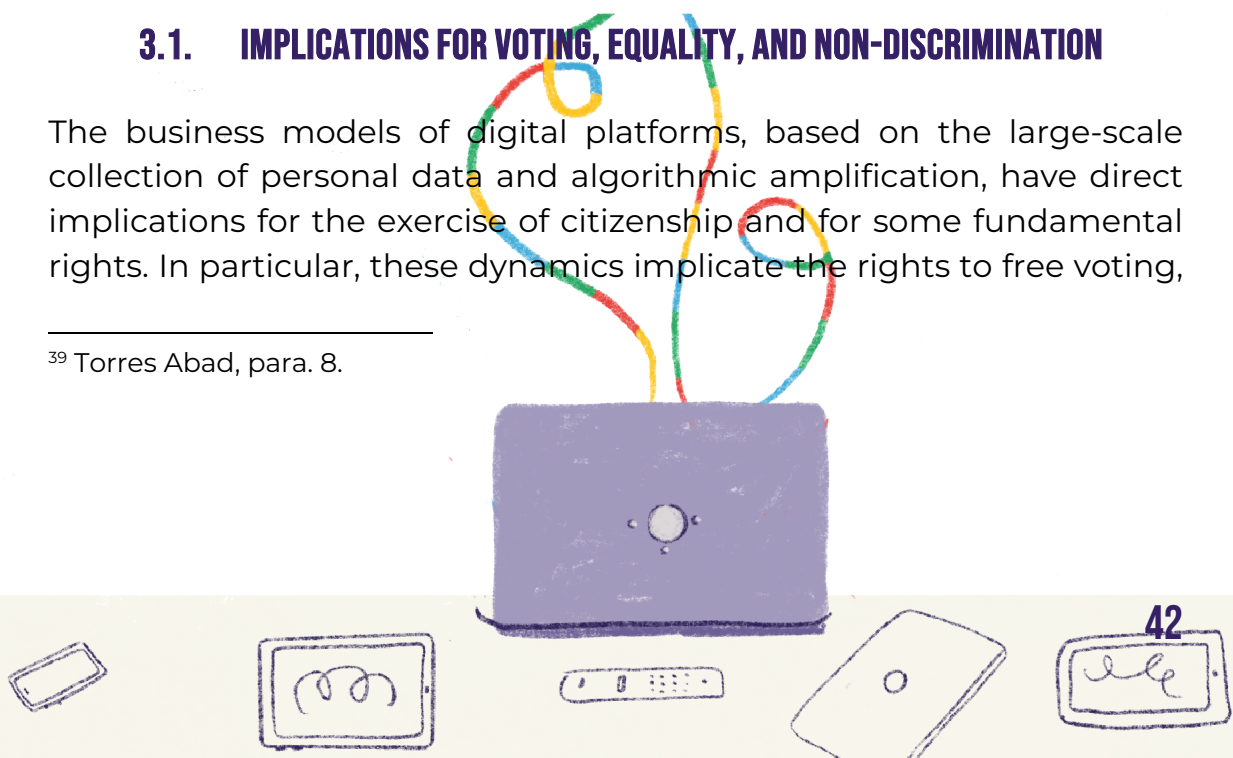
The AICR will not guarantee informational autonomy as recognized by the Inter-American Court and the Supreme Court, at least with regard to subsequent operations carried out in the United States with personal data exported from Argentina. Contrary to the position defended in Europe—and even for decades by the Argentine authorities themselves—that the United States poses general risks stemming from a lack of legal protection and the extension of jurisdiction, as well as specific risks arising from the application of the FISA Act, which authorizes the U.S. government to collect personal data sold by private companies for the purposes of state surveillance, the AICR classifies the United States as an “adequate jurisdiction.” As a result of this classification, data transfers to the United States will no longer be subject to the safeguards established by the Personal Data Protection Act, the model clauses, or the AAIP’s supervisory powers once the transfer is complete. Consequently, data subjects will see their ability to invoke the principle of consent—or to challenge the illegality, illegitimacy, or disproportionate nature of the uses that may be made of their data—reduced, if not eliminated, once their data is transferred to U.S. companies and/or from them to the U.S. federal government.

3. IMPACTS OF DATA-DRIVEN BUSINESS MODELS ON FUNDAMENTAL AND HUMAN RIGHTS

3.1. IMPLICATIONS FOR VOTING, EQUALITY, AND NON-DISCRIMINATION

The business models of digital platforms, based on the large-scale collection of personal data and algorithmic amplification, have direct implications for the exercise of citizenship and for some fundamental rights. In particular, these dynamics implicate the rights to free voting,

³⁹ Torres Abad, para. 8.

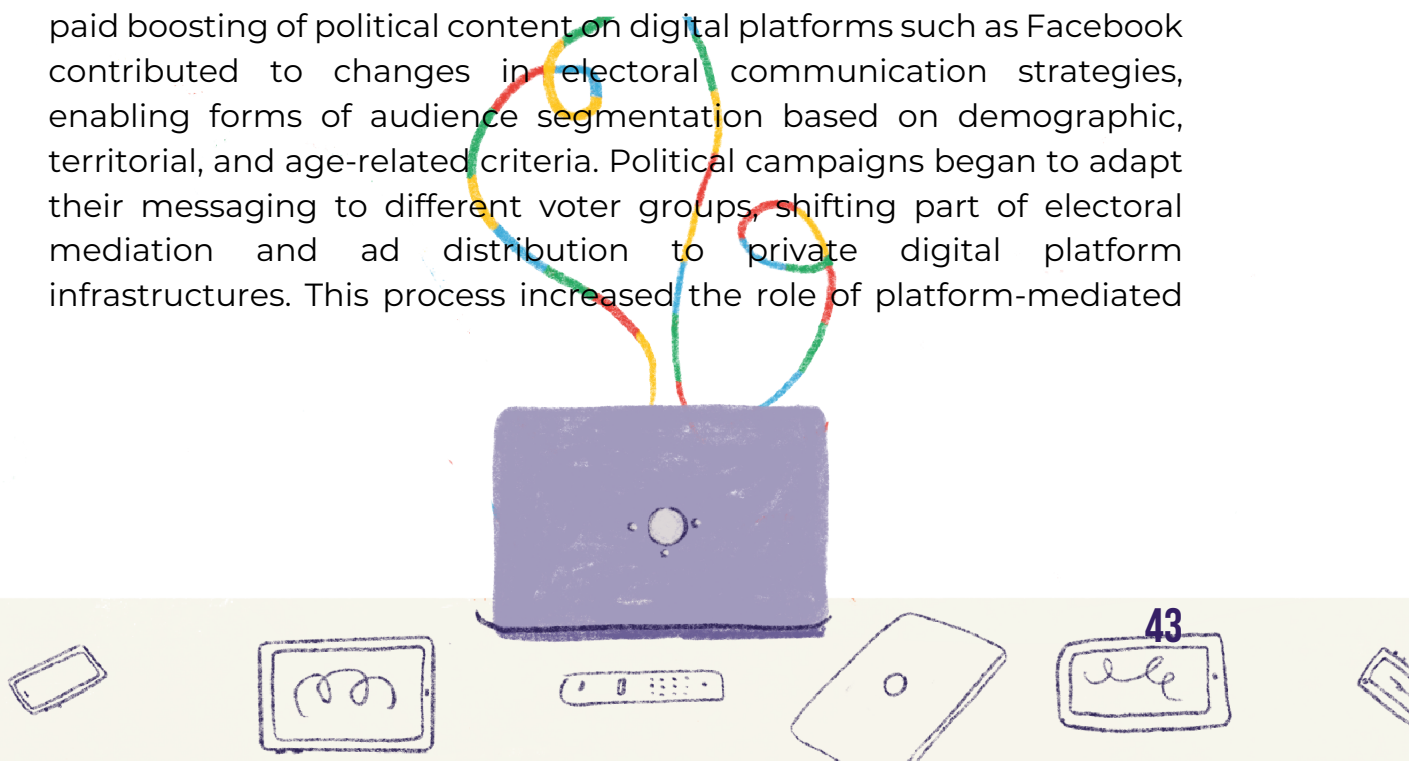


equality, and non-discrimination, as enshrined in Articles 23 and 24 of the American Convention on Human Rights (ACHR). This connection lies in the fact that the effective enjoyment of the right to vote depends not only on the formal ability to cast a ballot, but also on the existence of conditions that ensure free, informed, and equal participation in political and public life.

And over the past decade, electoral processes across the world, but also in our region, have unfolded in increasingly polarized and contentious public environments, characterized by the widespread circulation of disinformation, misinformation, hate speech, and online political violence. This context is further intensified by the business models and recommendation systems of digital platforms. The advancement of artificial intelligence tools capable of producing highly realistic synthetic content has also increased the challenges of protecting democratic public debate.

Political microtargeting is a practice that uses personal data, online behavior, and algorithmic inferences to segment voters and deliver highly tailored political messages to specific groups or individuals. It is enabled by the business models of digital platforms and based on their large-scale data collection. This new phenomenon has made electoral communication increasingly opaque and dependent on algorithmic infrastructures controlled by companies – a dynamic that gained global attention following the Cambridge Analytica case and its implications for democracy.

As an additional example, the problem of audience segmentation – and, in more advanced forms, microtargeting – in electoral communication could be observed in the 2018 Brazilian elections. The authorization of paid boosting of political content on digital platforms such as Facebook contributed to changes in electoral communication strategies, enabling forms of audience segmentation based on demographic, territorial, and age-related criteria. Political campaigns began to adapt their messaging to different voter groups, shifting part of electoral mediation and ad distribution to private digital platform infrastructures. This process increased the role of platform-mediated



targeting in electoral communication and raised concerns, especially regarding transparency.⁴⁰

Also, as previously highlighted in the document that substantiated the request for this hearing, the intersection of algorithmic profiling and digital electoral advertising has become one of the most significant threats to the integrity of democratic processes in Latin America. Figures from Colombia and Brazil⁴¹, for example, demonstrate that, on average, 70% of people rely on online information to form their political opinions. This complex context means that the formal guarantees of the right to vote, as we used to consider, are insufficient if they are not accompanied by material conditions that protect voters' informational autonomy. Creating scenarios that intentionally manipulate the information reaching voters, to disinform them, may undermine the basic principles of freedom of expression and informational pluralism.⁴²

It is equally important to highlight that with digital platforms and emerging technologies, the personalized and individualized dissemination of targeted electoral narratives becomes possible with remarkable ease, low cost, and limited transparency. Beyond prediction, these systems increasingly operate through the continuous shaping of perceptions and behaviors via tailored informational environments, particularly in contexts marked by unequal levels of digital literacy – according to 2023 data, only 28% of the population in Latin America has basic digital skills.⁴³

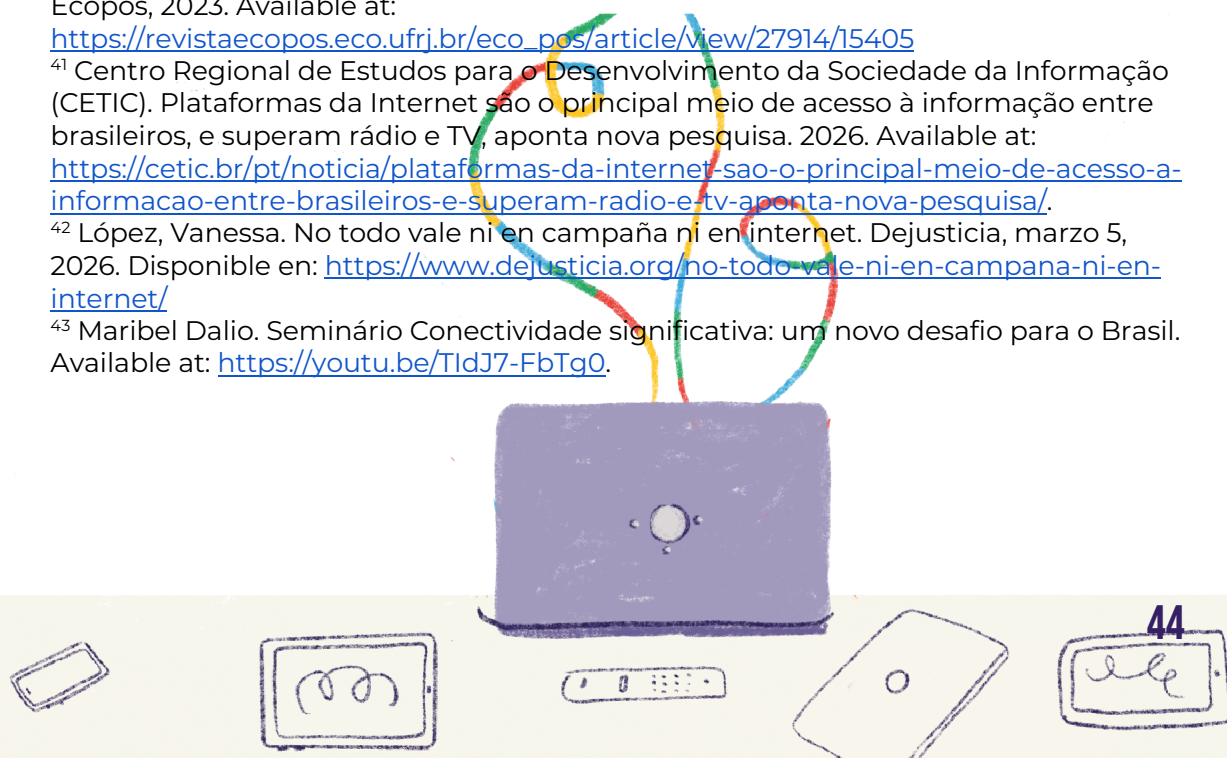
⁴⁰ Alves, Marcelo; Tavares, Camila. Propaganda eleitoral digital no Brasil: estratégias de segmentação de candidaturas à presidência em 2018 no Facebook. Revista Ecopós, 2023. Available at:

https://revistaecopos.eco.ufrj.br/eco_pos/article/view/27914/15405

⁴¹ Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC). Plataformas da Internet são o principal meio de acesso à informação entre brasileiros, e superam rádio e TV, aponta nova pesquisa. 2026. Available at: <https://cetic.br/pt/noticia/plataformas-da-internet-sao-o-principal-meio-de-acesso-a-informacao-entre-brasileiros-e-superam-radio-e-tv-aponta-nova-pesquisa/>.

⁴² López, Vanessa. No todo vale ni en campaña ni en internet. Dejusticia, marzo 5, 2026. Disponible en: <https://www.dejusticia.org/no-todo-vale-ni-en-campana-ni-en-internet/>

⁴³ Maribel Dalio. Seminário Conectividade significativa: um novo desafio para o Brasil. Available at: <https://youtu.be/TIdJ7-FbTg0>.

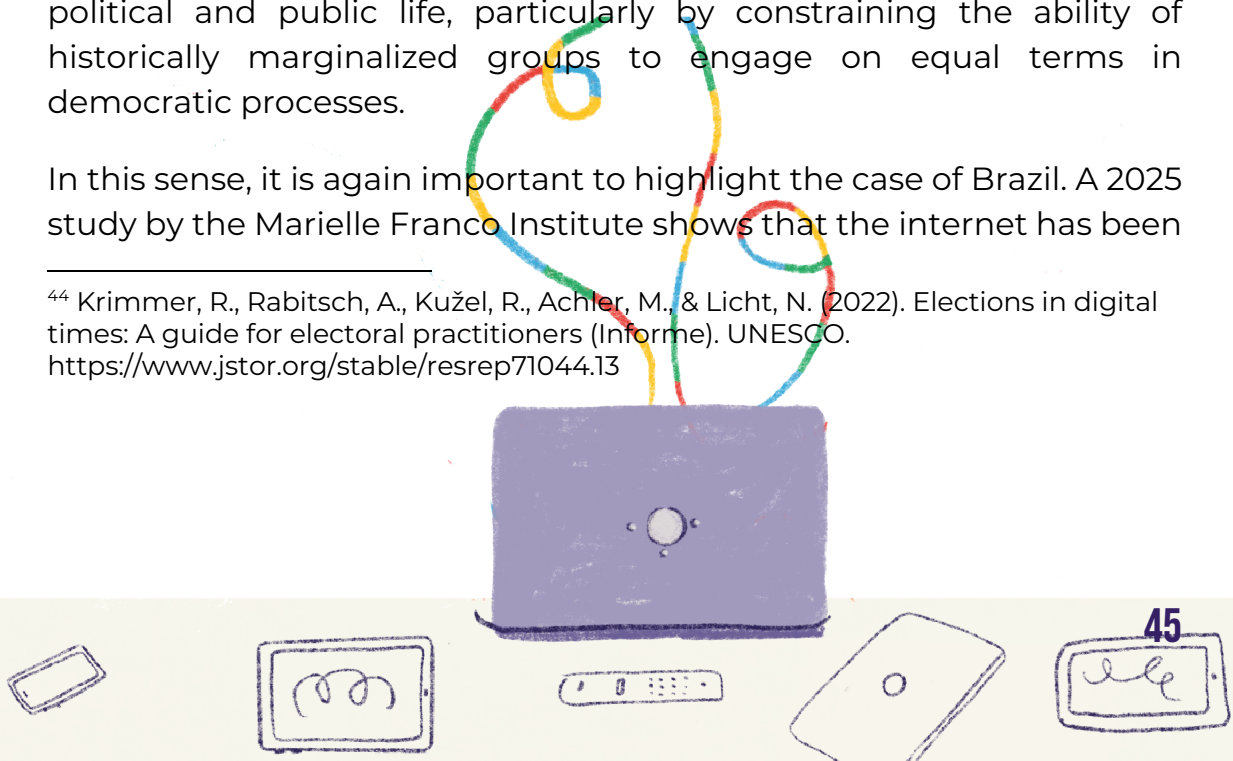


More than that, the concern with microtargeting is that it allows different groups to receive radically different messages about the same candidates or proposals, without any external actor being able to verify the content or scope of such communications. Likewise, “candidates and parties can make different promises or even contradictory statements to different groups of voters with little oversight or accountability.”⁴⁴ Those who possess the most comprehensive databases are social networks, as they enable profiling based on browsing history, social interactions, interests, and inferred vulnerabilities, potentially leading to informational distortion. This, in turn, produces significant asymmetries in electoral competition by granting unequal capacities to shape voter perceptions and tailor political communication. In sum, when combined with opaque targeting practices and unequal access to data-driven advertising infrastructures, such disparities may contribute to the reinforcement of structural imbalances between candidates and parties, raising concerns in relation to the abuse of economic and political power in digital campaigning environments.

Digital platforms’ recommendation systems and other algorithmic mechanisms, by amplifying the speed and reach of information flows, also tend to prioritize content that generates higher levels of attention and engagement. Because violent, polarizing, or emotionally charged content can elicit stronger reactions, it is often more likely to be amplified, recommended, and circulated by algorithmic systems operating within an economy of visibility. This dynamic facilitates the dissemination of harmful content and shapes the informational environment in which citizens form perceptions about public issues. In this context, it can affect the conditions for meaningful participation in political and public life, particularly by constraining the ability of historically marginalized groups to engage on equal terms in democratic processes.

In this sense, it is again important to highlight the case of Brazil. A 2025 study by the Marielle Franco Institute shows that the internet has been

⁴⁴ Krimmer, R., Rabitsch, A., Kužel, R., Achler, M., & Licht, N. (2022). Elections in digital times: A guide for electoral practitioners (Informe). UNESCO. <https://www.jstor.org/stable/resrep71044.13>



instrumentalized as a space for political violence aimed at hindering the political participation of women, activists, and elected representatives, particularly Black women and LGBTQIA+ individuals. Among the recorded cases of online violence, 71% consist of death and rape threats, often associated with discriminatory content and hate speech.⁴⁵ The MonitorA 2024 report also shows that such violence is systematic rather than episodic, disproportionately affecting women candidates, particularly Black women and LGBTQIA+ individuals. The report also notes cases of manipulated and altered content, including references to deepfakes and non-consensual synthetic sexual⁴⁶ content ('deepnudes'), as part of emerging trends in digital political violence. These dynamics are situated within electoral debate contexts, in which an intensification of violent interactions is observed during electoral cycles.⁴⁷ As can be inferred from the report produced by Terra de Direitos and Justiça Global, the growing impact of digital platforms on political contestation has given rise to a dual dynamic: while these platforms offer new opportunities for democratic participation, they also pose significant challenges to democracy by enabling the proliferation of hate speech, disinformation, and targeted attacks, thereby undermining the participation of certain groups in democratic processes.⁴⁸

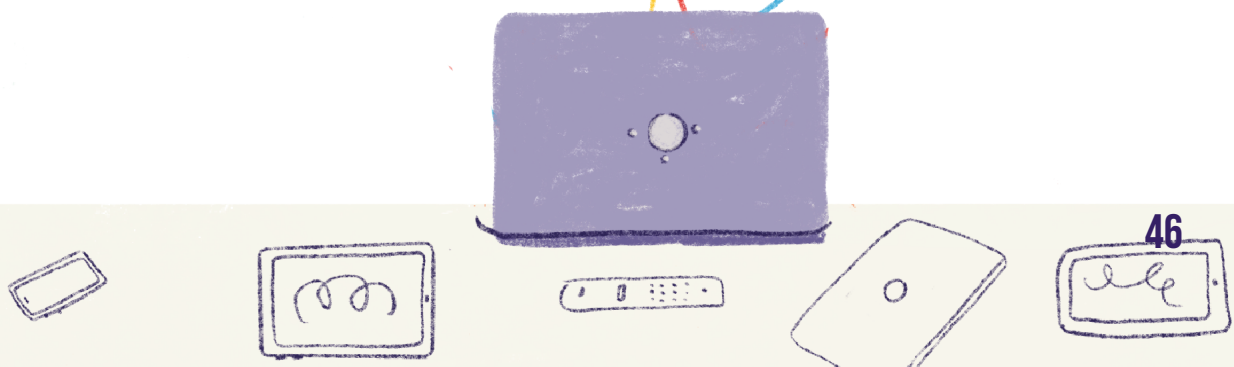
It is in this that online political violence operates as a structural mechanism that undermines political participation by producing exclusionary environments that constrain the full engagement of historically marginalized groups in democratic life. Rather than isolated content, this online violence is embedded in digital platform

⁴⁵ Instituto Marielle Franco. Regime de ameaça: violência política de gênero e raça no âmbito digital. 2025. Available at: <https://www.violenciapolitica.org/>.

⁴⁶ In this regard, UNICEF conducted a study in Colombia titled "Disrupting Harm: Technology-facilitated sexual exploitation and abuse of children and adolescents in Colombia." Available at: <https://www.unicef.org/colombia/informes/dirsupting-harm>

⁴⁷ Internetlab; Revista Azmina; Núcleo Jornalismo; LABHD UFBA. MonitorA: relatório sobre violência política contra candidatas(os) online. Edição 2024. São Paulo, 2025. Available at: https://internetlab.org.br/wp-content/uploads/2025/05/MonitorA-Relatorio_2024-3.pdf

⁴⁸ Justiça Global; Terra de Direitos. Violência política e eleitoral no Brasil. Panorama das violações de direitos humanos entre 1o de novembro de 2022 a 27 de outubro de 2024. Available at: https://www.global.org.br/wp/wp-content/uploads/2024/12/11-25_VIOLENCIA-POLITICA-2024-FN-2.pdf



engagement logics. Their dynamic can contribute to the amplification of harmful content targeting specific individuals' candidacies, as algorithmic systems may further distribute such material when it generates high levels of engagement, particularly when combined with prior audience segmentation based on behavioral data.

Another concern is the increasingly documented phenomenon of shadow banning. Recent studies suggest that people from historically marginalized groups (as racial and ethnic minorities, LGBTQ+ people, trans and/or nonbinary people) report experiences of shadow banning.⁴⁹ In practice, this means that digital platform architectures and algorithmic systems may reduce the visibility and reach of certain types of content, limiting the distribution of some messages through algorithmic suppression or reduced visibility. In the political sphere, these dynamics may disproportionately affect candidates from underrepresented groups, hindering their ability to reach voters, build name recognition, and compete on equal terms in digital campaign environments. As a result, voices that are already underrepresented in public debate may face additional barriers to political participation and representation.

Faced with this scenario, States in the region have the obligation to guarantee not only the right to vote as a formal act, but also the material conditions that make that vote truly free and informed. An electoral process in which citizens' personal data are used in a non-transparent manner to build political profiles, target differentiated messages, and amplify narratives containing disinformation and hate speech is not a process in which the freedom of voting is fully guaranteed.

The absence of accountability by major platforms regarding these practices consequently compromises not only individual rights to habeas data and information, but also the collective right to live in a democracy whose processes are genuinely sovereign and free from algorithmic interference.

⁴⁹ Risius, Marten; Blasiak, Kevin. Shadowbanning: an opaque form of content moderation. Available at: <https://espace.library.uq.edu.au/view/UQ:15cd999>.



3.2. PUBLIC DEBATE MANIPULATION: THE CASE OF BRAZIL'S BILL 2630

The risks described above are not limited to electoral advertising or the circulation of harmful content during campaigns. They also appear when dominant digital platforms use their own infrastructures, market position, and control over information flows to shape public debate about the rules that should govern them. A particularly illustrative example can be found in the Brazilian debate surrounding Bill 2630, commonly known as the “Fake News Bill.”

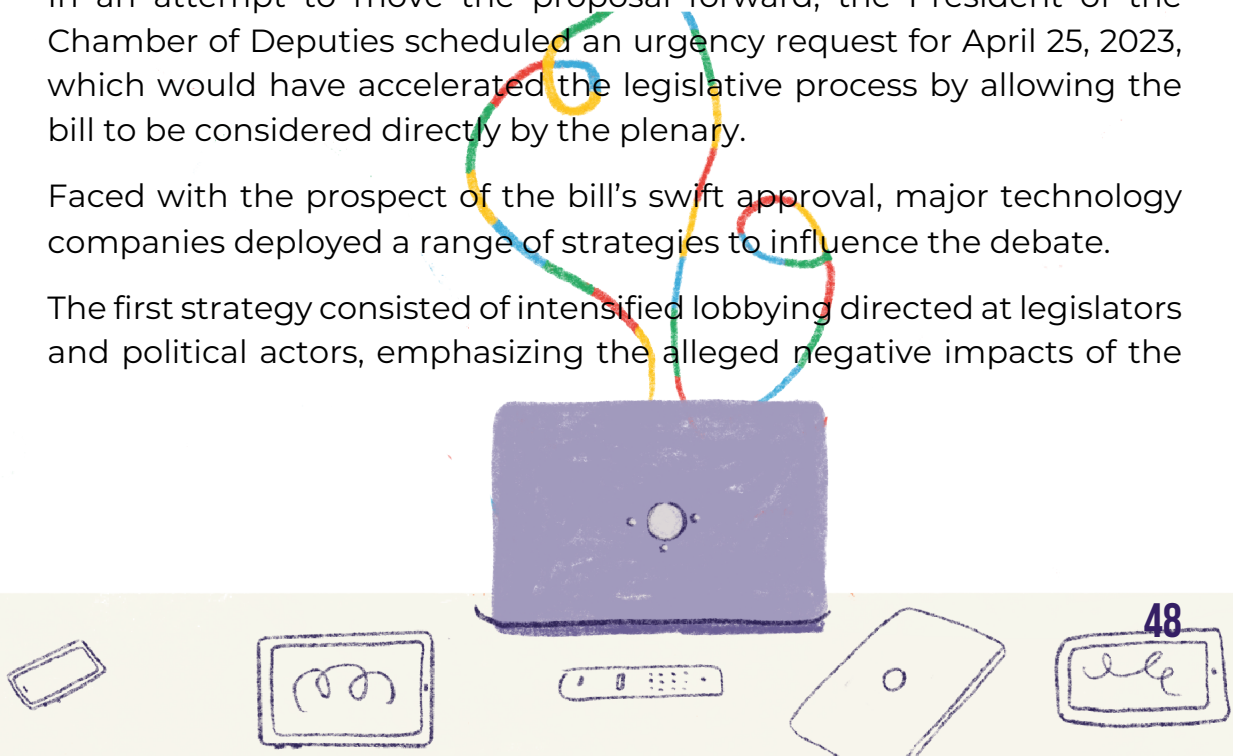
Bill 2630 was introduced in the Brazilian Senate in 2020. In its initial form, the proposal reflected, in part, a desire among some legislators to shield themselves from criticism in digital environments. However, the text became the object of extensive public debate and civil society engagement, which helped neutralize some of its most concerning provisions, including a proposed obligation to trace messages protected by end-to-end encryption.

After a new preliminary draft was released in early 2022, the bill remained stalled in the Chamber of Deputies until the beginning of 2023. In the aftermath of the failed attempt by far-right groups to overturn the newly inaugurated government of President Lula da Silva, and amid a peak in violent attacks in Brazilian schools, Bill 2630 became the main legislative vehicle for addressing broader concerns about the use of digital technologies in contexts of social unrest. To that end, the Executive Branch proposed a revised text to the bill's rapporteur, introducing several changes inspired by regulatory frameworks such as Germany's NetzDG, the European Union's Digital Services Act, and the United Kingdom's Online Safety Bill.

In an attempt to move the proposal forward, the President of the Chamber of Deputies scheduled an urgency request for April 25, 2023, which would have accelerated the legislative process by allowing the bill to be considered directly by the plenary.

Faced with the prospect of the bill's swift approval, major technology companies deployed a range of strategies to influence the debate.

The first strategy consisted of intensified lobbying directed at legislators and political actors, emphasizing the alleged negative impacts of the



Fake News Bill. A decisive element in the opposition campaign was the support obtained from the Evangelical Caucus, reportedly through coordinated lobbying led by Meta, which argued that obligations to prevent potentially illegal content could result in the removal of posts quoting biblical passages.⁵⁰

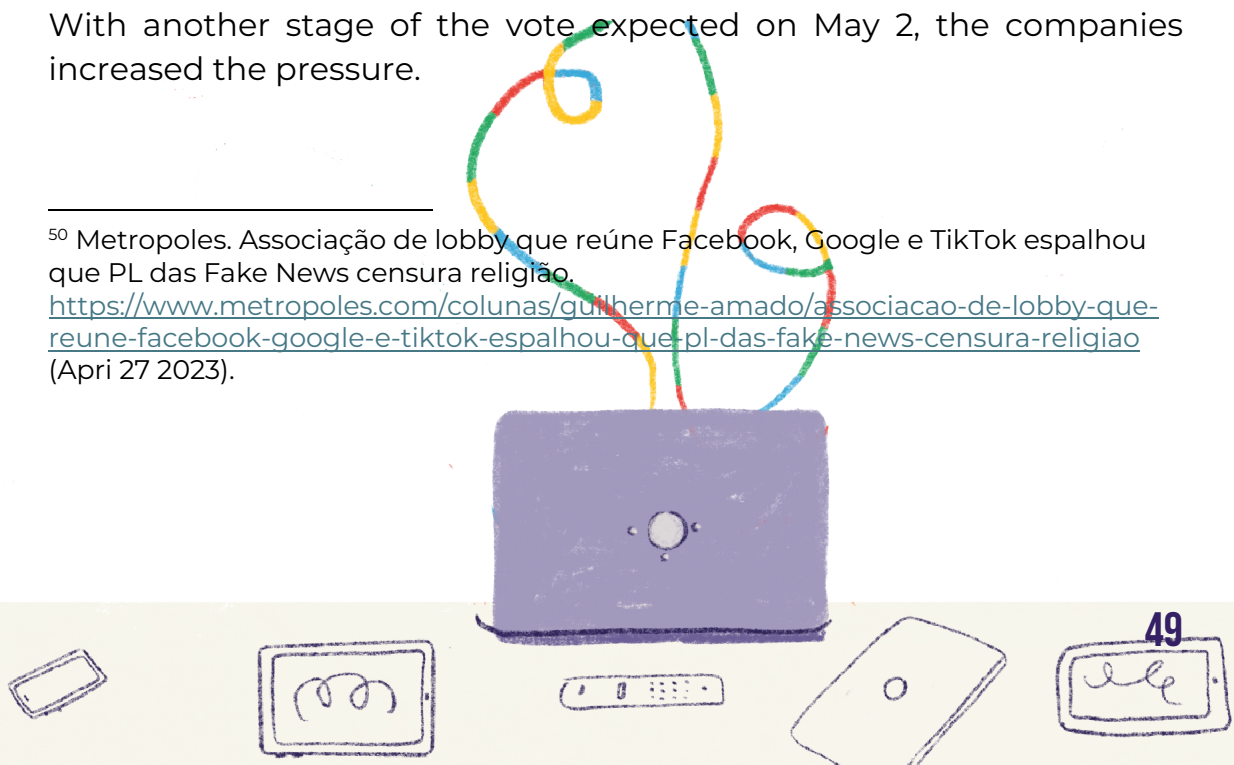
The economic power of these companies was central to the scale of the lobbying effort carried out in Congress. As reported by Agência Pública, Meta lobbyists were among the most frequent visitors to the Chamber of Deputies: Meta public policy managers Marconi Machado and André Atadeu each recorded more than one hundred visits between July 2022 and May 2025². Yet other strategies made even clearer how the concentration of economic power in digital platform markets can be used to steer public debate.

On the morning of April 25, 2023, the day the urgency request was scheduled for a vote, YouTube launched a campaign against Bill 2630 targeting content creators. The company argued that the proposal could give the government power to “control central aspects of the platform” and force it to “remove large amounts of legitimate content.”

The campaign was disseminated through the platform’s internal creator channels, by email, and on the company’s blog, encouraging the use of the hashtag #MaisDebate2630. YouTube also encouraged influencers to “make themselves heard,” resulting in videos that reproduced the company’s arguments. This strategy, which mobilized a group of people economically dependent on the platform to defend its corporate interests, strongly suggested that the companies’ participation in public debate would be shaped by the use of their economic power.

With another stage of the vote expected on May 2, the companies increased the pressure.

⁵⁰ Metropoles. Associação de lobby que reúne Facebook, Google e TikTok espalhou que PL das Fake News censura religião. <https://www.metropoles.com/colunas/guilherme-amado/associacao-de-lobby-que-reune-facebook-google-e-tiktok-espalhou-que-pl-das-fake-news-censura-religiao> (Apr 27 2023).



Between April 27 and May 2, Google reportedly invested more than R\$2 million in advertisements in print newspapers, television, and social media. In one advertisement alone, displayed between May 1 and May 3, Google paid Meta between R\$200,000 and R\$250,000 for a 15-second video claiming that Bill 2630 could increase confusion about what is true or false in Brazil. The video appeared more than one million times to users on Facebook and Instagram in Brazil. These advertisements were reportedly disseminated without being properly labeled as political campaigns, despite the platform's own rules requiring advertisers sponsoring content on social issues, elections, or politics to identify it as such.

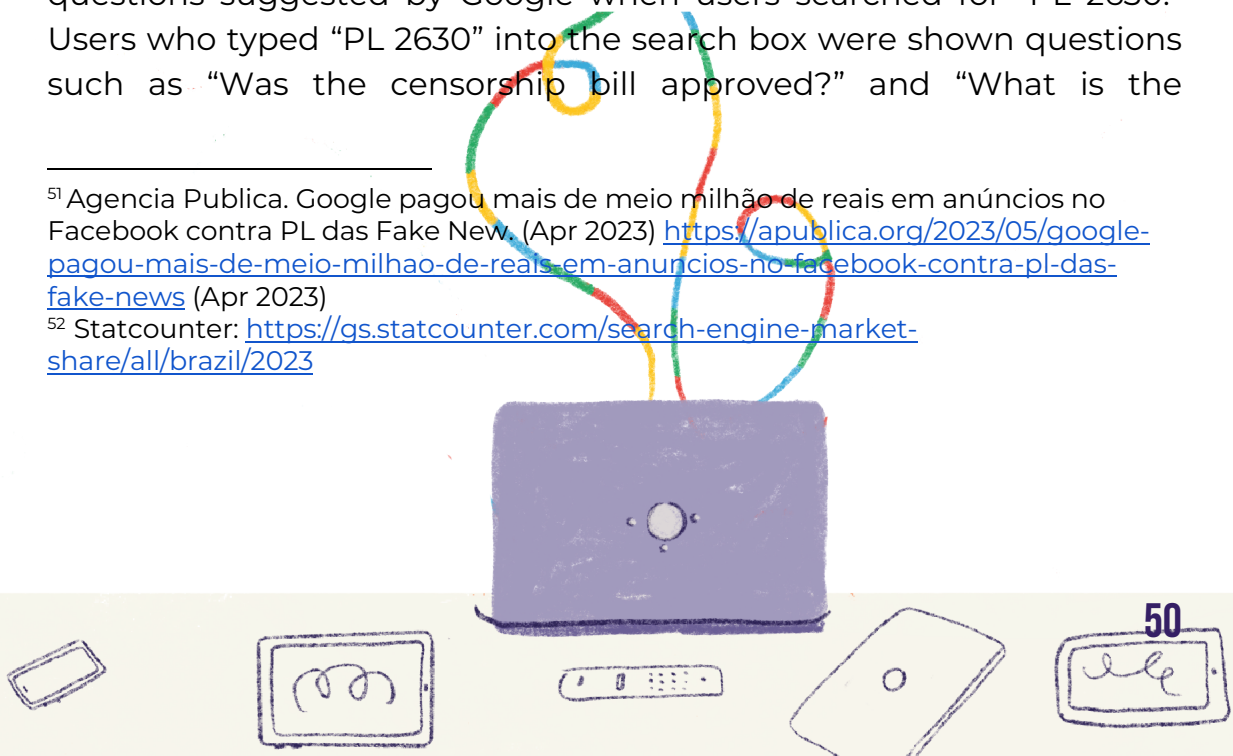
The scale of this investment is particularly revealing. Before the campaign against Bill 2630, Google's last recorded campaign on Facebook and Instagram had taken place in November 2022, during Black Awareness Month, when the company reportedly paid less than R\$100 and reached approximately 35,000 screens.⁵¹

On May 1, Google modified the design of its homepage to include a link opposing the bill. Users accessing the search engine saw, below the search box, the statement that "the Fake News Bill could increase confusion about what is true or false in Brazil." By clicking on the phrase, users were directed to Google posts defending the company's position against the bill. These messages were seen by millions of Brazilians, precisely because of Google's control over the search market: Google is the search engine used by approximately 86% of the 160 million Brazilians who use the internet.⁵²

Another action mapped by NetLab researchers concerned the alleged manipulation of search results. One example involved the related questions suggested by Google when users searched for "PL 2630." Users who typed "PL 2630" into the search box were shown questions such as "Was the censorship bill approved?" and "What is the

⁵¹ Agencia Publica. Google pagou mais de meio milhão de reais em anúncios no Facebook contra PL das Fake News. (Apr 2023) <https://apublica.org/2023/05/google-pagou-mais-de-meio-milhao-de-reais-em-anuncios-no-facebook-contra-pl-das-fake-news> (Apr 2023)

⁵² Statcounter: <https://gs.statcounter.com/search-engine-market-share/all/brazil/2023>



Censorship Bill?”—a pejorative term used by opponents of platform regulation, rather than the bill’s official name or the more common media label, “Fake News Bill.” Researchers considered this result significant because, according to data from Semrush, the most common Google queries related to Bill 2630 did not use the term “Censorship Bill.”⁵³

The research team also identified that the first result appearing for users seeking information about the bill was a sponsored post from Google’s own blog titled “learn about the Censorship Bill.”

Taken together, these actions illustrate how Google used its dominant position in the search market to shape users’ perceptions of the bill in a way that aligned with its commercial interests.

The pressure had measurable political effects. On April 26, 2023, 193 deputies opposed the bill and 236 supported it. Three days later, the balance had shifted: 228 deputies opposed the bill, 223 supported it, and 62 remained undecided. Shortly thereafter, the bill’s rapporteur decided to withdraw it from the agenda, and the proposal ultimately lost any realistic prospect of approval⁵⁴.

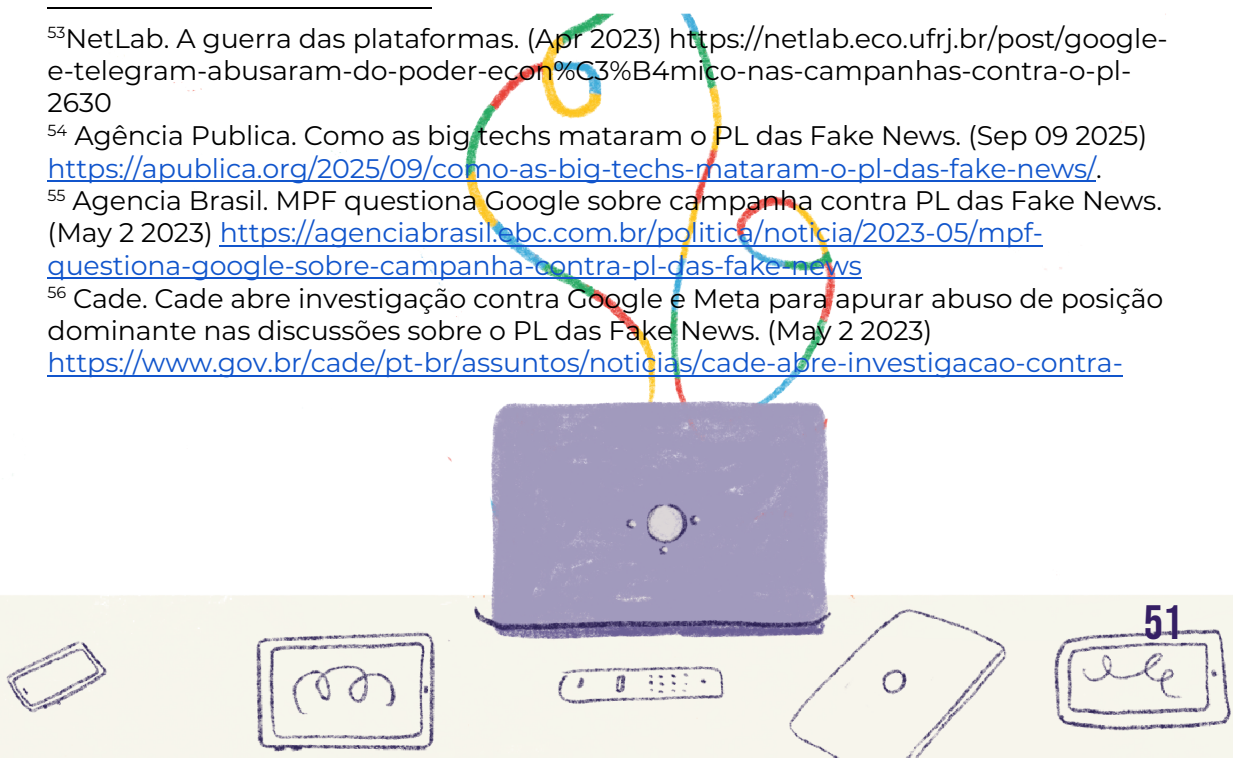
Some public authorities, including the Federal Public Prosecutor’s Office and the National Consumer Secretariat, sought to investigate the conduct of major technology companies in the campaign against the bill, particularly the possible abuse of economic power.⁵⁵ Brazil’s Administrative Council for Economic Defense also opened an administrative proceeding to examine alleged abuse of dominant position by Google and Meta in connection with the debates surrounding Bill 2630.⁵⁶ However, none of these initiatives resulted in

⁵³ NetLab. A guerra das plataformas. (Apr 2023) <https://netlab.eco.ufrj.br/post/google-e-telegram-abusaram-do-poder-econ%C3%B4mico-nas-campanhas-contra-o-pl-2630>

⁵⁴ Agência Pública. Como as big techs mataram o PL das Fake News. (Sep 09 2025) <https://apublica.org/2025/09/como-as-big-techs-mataram-o-pl-das-fake-news/>.

⁵⁵ Agência Brasil. MPF questiona Google sobre campanha contra PL das Fake News. (May 2 2023) <https://agenciabrasil.ebc.com.br/politica/noticia/2023-05/mpf-questiona-google-sobre-campanha-contra-pl-das-fake-news>

⁵⁶ Cade. Cade abre investigação contra Google e Meta para apurar abuso de posição dominante nas discussões sobre o PL das Fake News. (May 2 2023) <https://www.gov.br/cade/pt-br/assuntos/noticias/cade-abre-investigacao-contra->



meaningful accountability for the platforms or materially altered their capacity to use their own tools to influence public debate.

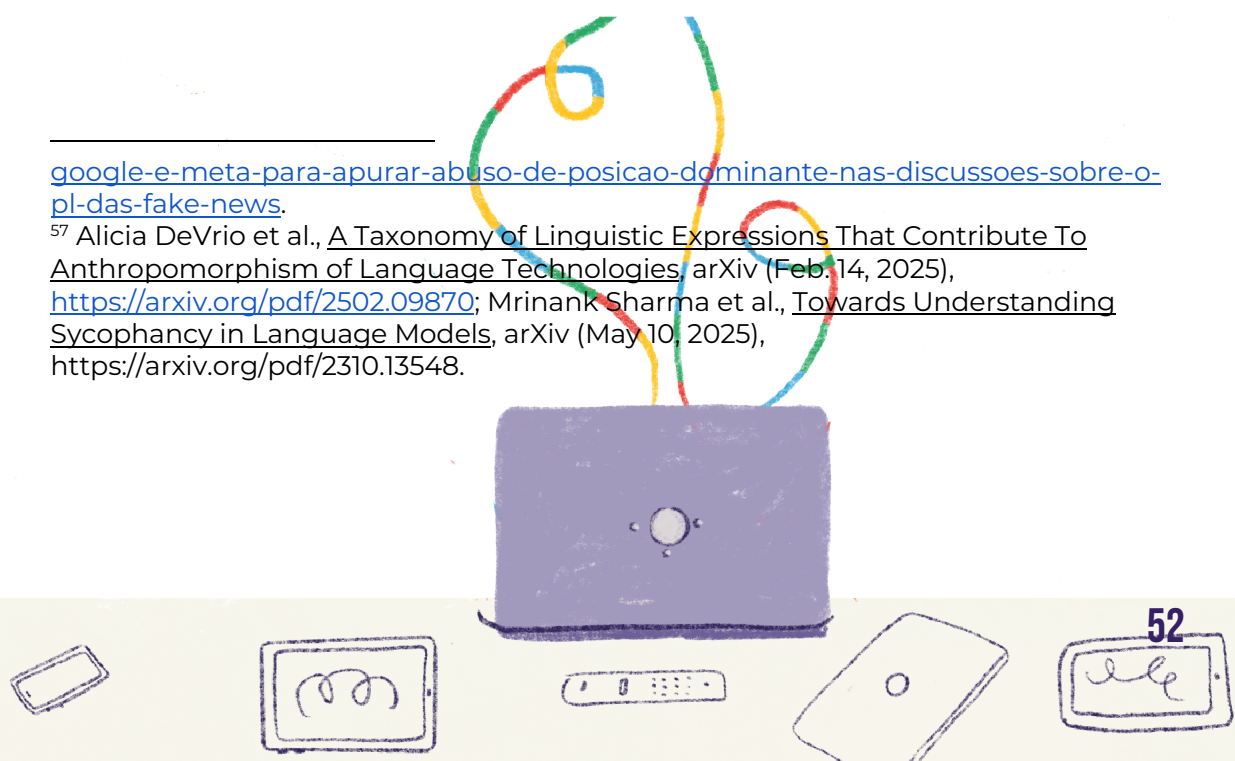
The relationship between the monopolistic position of major platforms and their ability to capture and manipulate public debate became particularly visible in the discussion around Bill 2630, but it has remained largely unchanged in recent years. Although Brazil has advanced new mechanisms for platform accountability, little has been done to reduce the economic power enjoyed by these companies. What the Brazilian experience reveals, therefore, is the absence of adequate instruments to address the concentration of economic power itself. For this reason, last year Brazil has begun discussing Bill 4675, which seeks to expand the powers of the competition authority so that it can respond to the new challenges posed by digital markets and the conduct of large technology companies.

3.3. MENTAL HEALTH EFFECTS PRIMARILY RELATED TO GENERATIVE AI PLATFORMS

The advent of generative AI products has deepened the threat that addictive design poses to human rights in the Americas. Generative AI chatbots, which are powered by Large Language Models (LLMs), are sophisticated conversational agents programmed to synthesize entirely new, context-aware responses by predicting words based on massive training datasets. As a result, the outputs of LLM-chatbots mimic human speech and generate responses that affirm their users.⁵⁷ These design features of anthropomorphism and sycophancy have led many consumers to experience both general-purpose chatbots such as ChatGPT and companion chatbots such as Character.AI as confidants

[google-e-meta-para-apurar-abuso-de-posicao-dominante-nas-discussoes-sobre-o-pl-das-fake-news.](#)

⁵⁷ Alicia DeVrio et al., A Taxonomy of Linguistic Expressions That Contribute To Anthropomorphism of Language Technologies, arXiv (Feb. 14, 2025), <https://arxiv.org/pdf/2502.09870>; Mrinank Sharma et al., Towards Understanding Sycophancy in Language Models, arXiv (May 10, 2025), <https://arxiv.org/pdf/2310.13548>.



with unlimited availability who always agree with them, encouraging excessive use and dependence.⁵⁸

Additionally, like social media platforms, many chatbots collect extensive data about individual users and use that data to personalize chatbot responses through features such as ChatGPT's "Memory" to more effectively engage users, keeping them online longer.⁵⁹ User data is also used to train AI models to make chatbots even more effective at simulating human speech.⁶⁰ Because of chatbots' warm, human-like responses, consumers tend to include more intimate data about themselves in their messages, which increases AI companies' ability to exploit their personal data to increase engagement.⁶¹

The combination of sycophantic, human-like design and features that exploit personal data to personalize user experience has proven highly effective. As of February 2026, one in four U.S. adults use generative AI chatbots every day.⁶² Children and people with disabilities appear particularly vulnerable to AI chatbots' addictive features. More than half of teens use chatbots, with three in ten using them daily and 16% using chatbots several times per day or "almost constantly."⁶³ More than one third of U.S. psychologists report that they have patients turning to AI chatbots as an additional mental health professional.⁶⁴

⁵⁸ Zilan Qian et al., Mapping the Parasocial AI Market: User Trends, Engagement and Risks, arXiv (Jul. 22, 2025), <https://arxiv.org/pdf/2507.14226>.

⁵⁹ E.g., Dreaming: Better Memory for a More Helpful ChatGPT, OpenAI (June 4, 2026), <https://openai.com/index/chatgpt-memory-dreaming/>.

⁶⁰ Nikki Goth Itoi, Be Careful What You Tell Your AI Chatbot, Stanford University Center for Human-Centered Artificial Intelligence (Oct. 15, 2025), <https://hai.stanford.edu/news/be-careful-what-you-tell-your-ai-chatbot>.

⁶¹ Muhammad Jazlan, Tracking Conversations: Measuring Content and Identity Exposure on AI Chatbots, arXiv, 1 (May 13, 2026), <https://arxiv.org/pdf/2604.27438>.

⁶² Gottfried et al., Americans and AI 2026: Chatbots, Smart Devices and Views on Impact, Pew Research Center (June 17, 2026), <https://www.pewresearch.org/internet/2026/06/17/americans-and-ai-2026-chatbots-smart-devices-and-views-on-impact>

⁶³ Michelle Faverio & Olivia Sidoti, Teens, Social Media and AI Chatbots 2025, Pew Research Center, <https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/#frequency-of-chatbot-use>.

⁶⁴ Patients are bringing AI to therapy: Highlights from the 2026 Chatbots and Mental Health Survey, American Psychological Association (2026), <https://www.apa.org/pubs/reports/chatbots-mental-health-2026>.



The addictive design of AI chatbots has devastating effects on consumers' mental health and human rights, particularly for children and people with disabilities. In the United States, multiple lawsuits have been filed concerning individuals who died by suicide after intense periods of chatbot usage, during which the AI product affirmed or encouraged suicidality.⁶⁵ Other individuals have developed debilitating delusions after being persuaded by an AI chatbot that increasingly severe delusions are true.⁶⁶ Previously high-functioning individuals who have developed AI delusions have attempted and committed murder,⁶⁷ lost jobs and amassed financial debt,⁶⁸ and experienced psychic breaks so severe they are unable to identify loved ones.⁶⁹ Even consumers who escape these extreme mental health impacts experience negative psychological effects, as the use of AI chatbots has been associated with a decline in cognitive abilities.⁷⁰

These impacts on the psyche threaten the human rights of all people, especially children, adolescents, people with mental disabilities, and others with heightened vulnerability to generative AI risks. Article 13 protects the human right to freedom of thought, a non-derogable right that includes freedom from indoctrination and manipulation of thought.⁷¹ Generative AI chatbots encroach on this freedom through

⁶⁵ E.g., Garcia v. Character Technologies, 6:24-cv-01903 (M.D. Fl. Oct. 22, 2024); Shamblin v. OpenAI, Inc., Case No. 25STCV32382 (Super. Ct. Cal. Cnty. L.A., Nov. 6, 2025); Fox v. OpenAI, Inc., Case No. 25STCV32379 (Super. Ct. Cal. Cnty. L.A., Nov. 6, 2025)

⁶⁶ Luke Nicholls, et al., “AI Psychosis” in Context: How Conversation History Shapes LLM Responses to Delusional Beliefs, arXiv (June 1, 2026), <https://arxiv.org/pdf/2604.13860>.

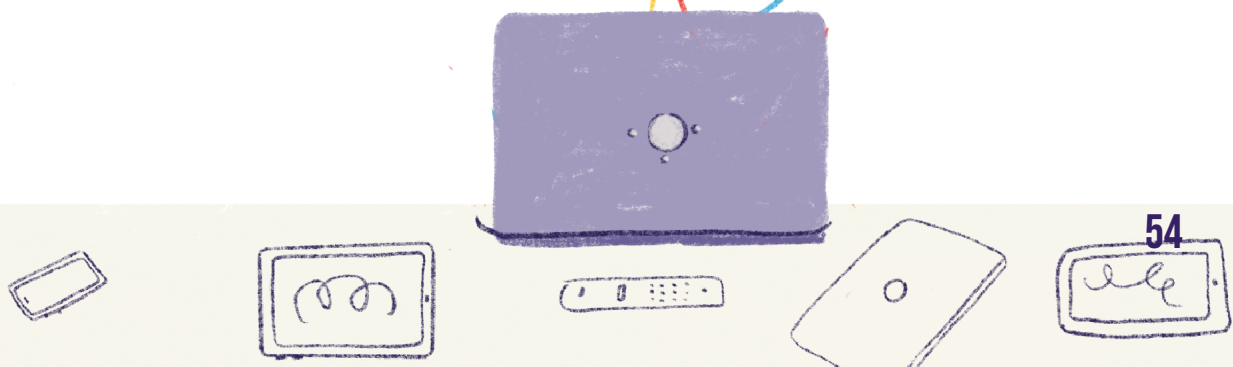
⁶⁷ Katyanna Quach, AI girlfriend encouraged man to attempt crossbow assassination of Queen, The Register (Oct. 6, 2023), <https://www.theregister.com/software/2023/10/06/ai-chatbot-encouraged-man-to-kill-the-queen-court-hears/1370624> (attempted assassination of Queen of England); First Cnty. Bank v. OpenAI Foundation, Case No. CGC-25-631477 (Super. Ct. Cal. Cnty. S.F., Dec. 11, 2025) (murder committed).

⁶⁸ Madden v. OpenAI, Inc., Case No. 25STCV32383 (Super. Ct. Cal. Cnty. L.A., Nov. 6, 2025).

⁶⁹ Compl., Fox, Case No. 25STCV32379, at *9.

⁷⁰ Nataliya Kosmyrna et al., Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task, arXiv (June 2025), <https://arxiv.org/pdf/2506.08872v1#page=141.78>.

⁷¹ Susie Alegre, Rethinking Freedom of Thought for the 21st Century, 3 Eur. Hum. Rts. L. Rev. 221, 227-27 (2017),



their demonstrated capability to manipulate thoughts and to inhibit their users' ability to freely and independently formulate their own thoughts. This threat creates an obligation on states to act to ensure the fulfillment of individuals' right to freedom of thought.⁷² OAS member states are not currently realizing this obligation because they are failing to adequately regulate generative AI and have not imposed restrictions on generative AI companies that sufficiently protect against interference with the right to freedom of thought.⁷³

Generative AI chatbots additionally threaten the right to private life, the right to informational self-determination, and the right to dignity. The recognition of dignity in the American Convention entails "the possibility, accorded to all human beings, of self-determination and to freely choose the options and circumstances that give meaning to their existence based on their own preferences and convictions."⁷⁴ But the exceptional manipulative capabilities of generative AI chatbots prevent individuals from freely choosing their circumstances, as their capacity for free choice is inhibited by acute delusions, depressive spirals, and/or cognitive decline. This threat is manifest in the cases brought so far in United States courts. For example, one woman has alleged that she was proud of her career at a technology company but, after developing AI-fueled delusions, she quit and became immersed in an AI-generated fantasy that she was not human and her debt would be eliminated by

<https://www.doughtystreet.co.uk/sites/default/files/media/document/Rethinking%20Freedom%20of%20Thought%20for%20the%2021st.pdf>; Ahmed Shaheed (Special Rapporteur on Freedom of Religion or Belief), *Interim Rep.: Freedom of Thought*, ¶¶ 35-39, U.N. Doc. A/76/389 (Oct. 5, 2021), <https://docs.un.org/en/A/76/380>.

⁷² Shaheed, *supra* note 15, at ¶ 97 (including recommendations to States that would protect against encroachment on the right to freedom of thought by private actors); Jan Christoph Bublitz, *Freedom of Thought and Digital Technologies: Operationalizing State Obligations for Social Media, Virtual Reality, and Neurotechnology*, 26 Hum. Rts. Rev. 313 (Nov. 22, 2025), <https://link.springer.com/article/10.1007/s12142-025-00751-0#Sec11>.

⁷³ See *AI Watch: Global Regulatory Tracker*, White & Case, <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker#home>.

⁷⁴ *Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia*, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 506, ¶ 569 (Oct. 18, 2023).



divine forces.⁷⁵ Generative AI interfered with her fundamental capacity to self-determine.

Furthermore, generative AI companies are increasingly turning to business models familiar from social media, where individuals' personal data is exploited and shared with third parties for profit.⁷⁶ This conduct appears to contravene the Updated Principles on Privacy and Personal Data Protection and Inter-American jurisprudence on the right to informational self-determination, which protects individuals against private as well as state encroachment.⁷⁷ Because of the emotional dependence AI chatbots cultivate, the data collected by individuals who use chatbots is likely to include sensitive content about their innermost thoughts and beliefs, raising particular concern about the exploitation of this data.

3.4. IMPLICATIONS FOR CHILDREN'S RIGHTS

3.4.1. ALGORITHMIC CONTENT RECOMMENDATION SYSTEMS MUST BE RECOGNIZED AS AN INTEGRAL COMPONENT OF THE ADDICTIVE DESIGN OF SOCIAL MEDIA.

The additive design of digital applications, especially social networks, is also composed of algorithmic content recommendation systems, which are added to other design patterns such as infinite scrolling, autoplay and rewards for time of use to maximize user engagement. On social networks, these algorithms infer behavioral preferences

⁷⁵ Madden, Case No. 25STCV32383, at 4-10.

⁷⁶ Muhammad Jazlan et al., Tracking Conversations: Measuring Content and Identity Exposure on AI Chatbots, arXiv (May 13, 2026), <https://arxiv.org/pdf/2604.27438>.

⁷⁷ Organization of American States, Updated Principles on Privacy and Personal Data Protection, 12-14, OEA/Ser.D/XIX/20 (Jan. 3, 2022), https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf; Members of the “José Alvear Restrepo” Lawyers Collective v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 506, ¶ 570 (Oct. 18, 2023) (“people are also free to exercise self-determination to decide when and how much to reveal matters of their personal lives, which includes defining what type of information, including their personal data, may be known by others”).



through the processing of personal data collected from users during their browsing, and suggest new content of potential interest to them⁷⁸.

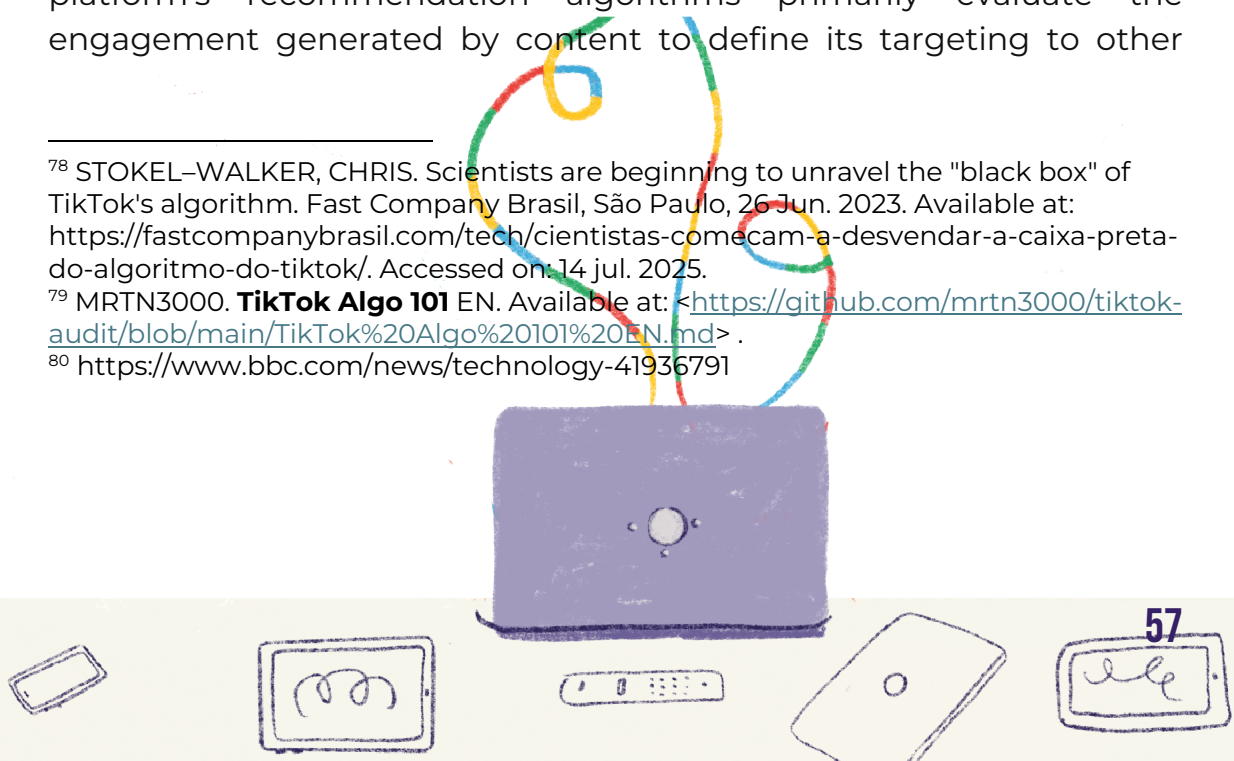
With this, a continuous and highly personalized flow of content is created, often conveyed in the format of short videos, in a model that feeds back: as users receive this content and interact (or not) with it, these interactions are metricated and converted into behavioral data, used to guide the recommendation of new content. The longer the user stays on the platform, therefore, the more data about them is collected and the more effective their algorithmic systems become in targeting content that can increase engagement.

The above is corroborated by several internal documents, produced by the social media providers themselves, which have been made public over the past few years. In December 2021, Ben Smith, a journalist for the American newspaper The New York Times, published the article How TikTok Reads Your Mind, in which he exposed information extracted from a document entitled TikTok Algo 101⁷⁹, produced by ByteDance's own team of engineers in Beijing. The document, whose authenticity was later confirmed by the company, was leaked by a confidential source, and exposed that TikTok's algorithms are designed with the aim of retaining the app's users (an indicator referred to as "retention") and increasing their usage time. With regard to Meta, in 2017, the company's then-CEO, Sean Parker, stated that "the thought process that went into building these applications, Facebook being the first of them, ... was all about: 'How do we consume as much of your time and conscious attention as possible?'.⁸⁰ The comments made almost a decade ago reflect what Adam Mosseri, current CEO of Instagram (a product offered by Meta) in 2025, exposed: according to him, the platform's recommendation algorithms primarily evaluate the engagement generated by content to define its targeting to other

⁷⁸ STOKEL-WALKER, CHRIS. Scientists are beginning to unravel the "black box" of TikTok's algorithm. Fast Company Brasil, São Paulo, 26 Jun. 2023. Available at: <https://fastcompanybrasil.com/tech/cientistas-comecam-a-desvendar-a-caixa-preta-do-algoritmo-do-tiktok/>. Accessed on: 14 jul. 2025.

⁷⁹ MRTN3000. **TikTok Algo 101** EN. Available at: <<https://github.com/mrtn3000/tiktok-audit/blob/main/TikTok%20Algo%20101%20EN.md>> .

⁸⁰ <https://www.bbc.com/news/technology-41936791>



users, based on metrics such as user interaction time, the number of people who saved it and shared it with others⁸¹.

The evidence shows that the algorithms of social media platforms popular among children are trained and calibrated based on parameters strictly aimed at retention and the extension of the user's usage time; and not at the well-being of users or the creation of a healthy and diverse informational ecosystem in the process of disseminating content.

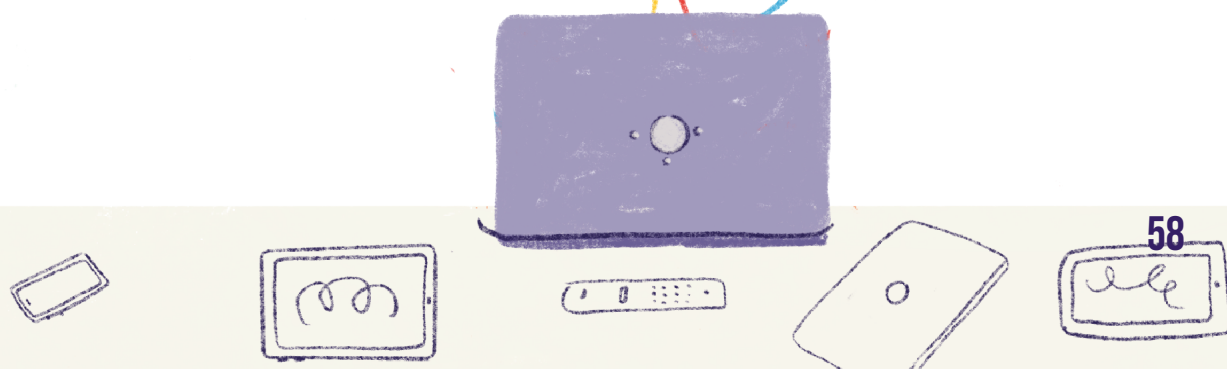
The recognition of the role of algorithmic content recommendation systems in the additive design of social networks is relevant to the extent that it negatively affects the quality of the content that children have access to on these platforms. By adopting indicators strictly related to engagement as a central parameter for boosting content, the algorithms that operate in them end up expanding the reach of content that puts the rights and well-being of users in check, especially children, as well as inserting them into self-referential spirals that can aggravate preexisting behavioral and mental health issues.

In order to understand why the incessant search for attention retention interferes with the quality of content offered to consumers by algorithmic recommendation systems, it is convenient to use as a starting point the considerations made by the Attorney General of Massachusetts in the lawsuit he filed against ByteDan⁸²ce⁸³, the result of a careful analysis of several internal documents of the company unveiled in the investigation processes conducted by the FTC:

⁸¹ Deshpande, V. (2025, December 24). *How Instagram ranks posts: Adam Mosseri breaks down the algorithm*. PitchONNET. <https://www.pitchonnet.com/pitch-feature/how-instagram-ranks-posts-adam-mosseri-breaks-down-the-algorithm-38374.html>

⁸² It is worth noting that a study on mental health and digital environments published by the OECD in 2026 presented evidence regarding a sense of loss of control among 62% of students across 15 of the organization's member countries. For further details, see: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/growing-up-in-the-social-media-age_be0c75c6/a1132839-en.pdf

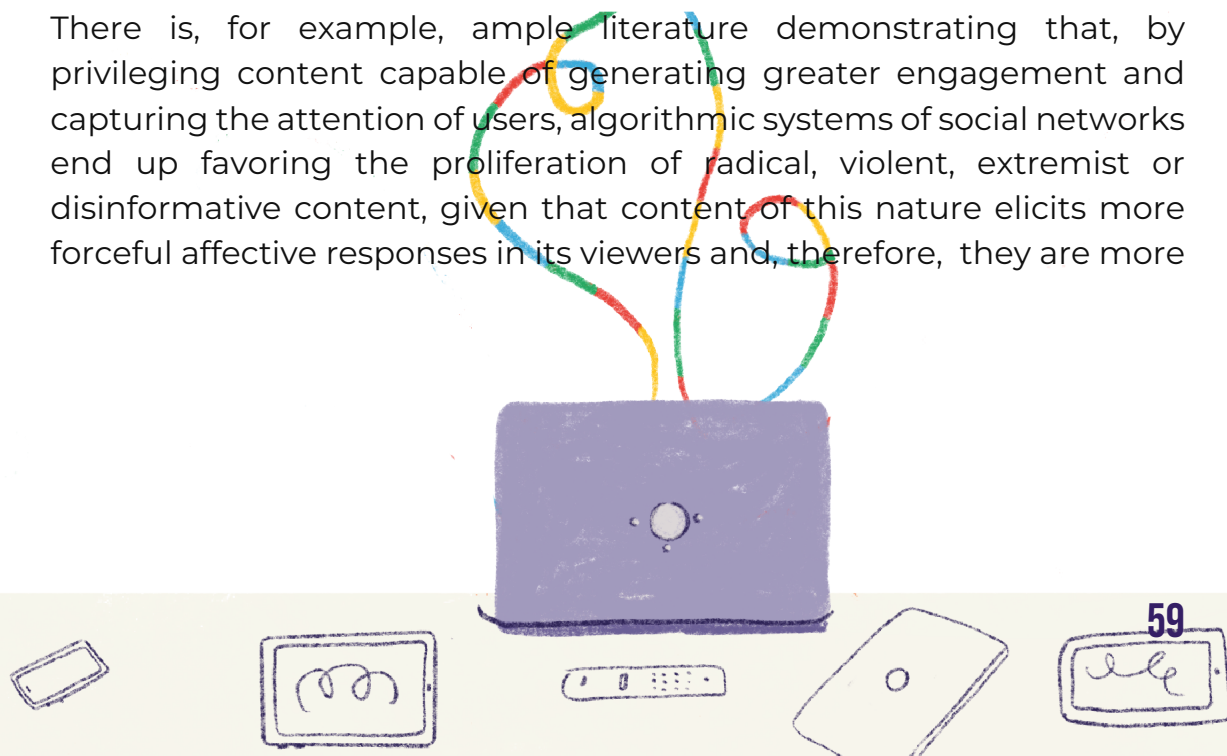
⁸³ Office of the Attorney General of Massachusetts. (2024, October 8). *Commonwealth of Massachusetts v. TikTok Inc. et al.: Complaint* [Legal complaint]. <https://www.mass.gov/doc/tiktok-complaint-unredacted/download>



TikTok's recommendation system is content-indifferent or, in TikTok's own words, "content-neutral," meaning it "recommends videos to users based on user and community behavior, regardless of the content." As described in an internal TikTok document, the "algorithm doesn't care about content — it doesn't have an agenda. It doesn't qualitatively understand" the content he shows to users. Another internal document, the screenshot of which is below, also defends the "content-neutral" nature of TikTok's recommendation system, as it "recommends content based on behavior and certain device signals rather than the semantic nature of the content itself," "does not promote or suppress specific agendas, views, or content," and "does not 'understand' the content. (paragraph 161)

Therefore, according to the Attorney General, the recommendation of videos by TikTok's algorithmic systems is based not on semantic considerations regarding their content, but rather on the engagement metrics captured by the platform from their use; what ByteDance refers to as "neutrality". This supposed neutrality, however, has nothing neutral about it, since the adoption of parameters related to user retention for content targeting directly interferes with the type of content whose promotion will be favored, favoring the dissemination of videos that present certain values, languages and messages to the detriment of others. In other words: this alleged split between evaluative analysis of the semantic content of short videos and analysis of their engagement potential is only illusory.

There is, for example, ample literature demonstrating that, by privileging content capable of generating greater engagement and capturing the attention of users, algorithmic systems of social networks end up favoring the proliferation of radical, violent, extremist or disinformative content, given that content of this nature elicits more forceful affective responses in its viewers and, therefore, they are more



apt to retain your attention⁸⁴. Other studies show that social media algorithms contribute to the crystallization of aesthetic standards that subjugate girls and women⁸⁵, as well as to the reaffirmation of racism with the invisibility of black people's bodies and voices⁸⁶.

In addition, informed by the massive processing of personal data and guided by the logic of personalization, algorithmic recommendation systems acquire the power to exploit users' vulnerabilities in order to keep them engaged. Linked solely to the purpose of capturing attention, recommendation algorithms operate from a logic that does not reject, at least a priori, inappropriate content or content that violates the rights of children, as long as this content is capable of meeting the commercial objectives unilaterally determined by the companies providing these services.

Videos that promote eating disorders or romanticize depressive conditions, for example, will not necessarily fail to be boosted by social media algorithms if they contribute to their goal of expanding engagement and retaining attention, regardless of the illegality of their content or their impacts on younger users. On the contrary, there are indications that they will be actively targeted to consumers whose behavior indicates that this targeting will imply greater interest and expenditure of time on the platform.

Thus, what is referred to as neutrality could be better described as indifference and omission in relation to the well-being and rights of child and adolescent users. In the name of maintaining engagement

⁸⁴ Vide: BRADY, William J. MCLOUGHLIN, Killian L. **Human-algorithm interactions help explain the spread of misinformation**. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S2352250X23002154>>. Acesso em 22 nov. 2025.

⁸⁵ CHARLITA DE FREITAS, Luciano. **Aesthetic gender standardization in Artificial Intelligence algorithms: a case study on the Instagram app**. Internet & Society – InternetLab. Available at: <<https://revista.internetlab.org.br/normatizacao-estetica-de-genero-em-algoritmos-de-inteligencia-artificial-estudo-de-caso-sobre-o-aplicativo-instagramnota-id1/>>. Accessed on: 17 jul. 2025.

⁸⁶ CARNEIRO, Giovanna. **Racist algorithm explains why content produced by black people earns less on YouTube**. Marco Zero Content. Published on: 05 Nov. 2024. Available at: <<https://marcozero.org/algoritmo-racista-explica-por-que-conteudo-produzido-por-negros-fatura-menos-no-youtube/>>. Accessed on: 17 jul. 2025.



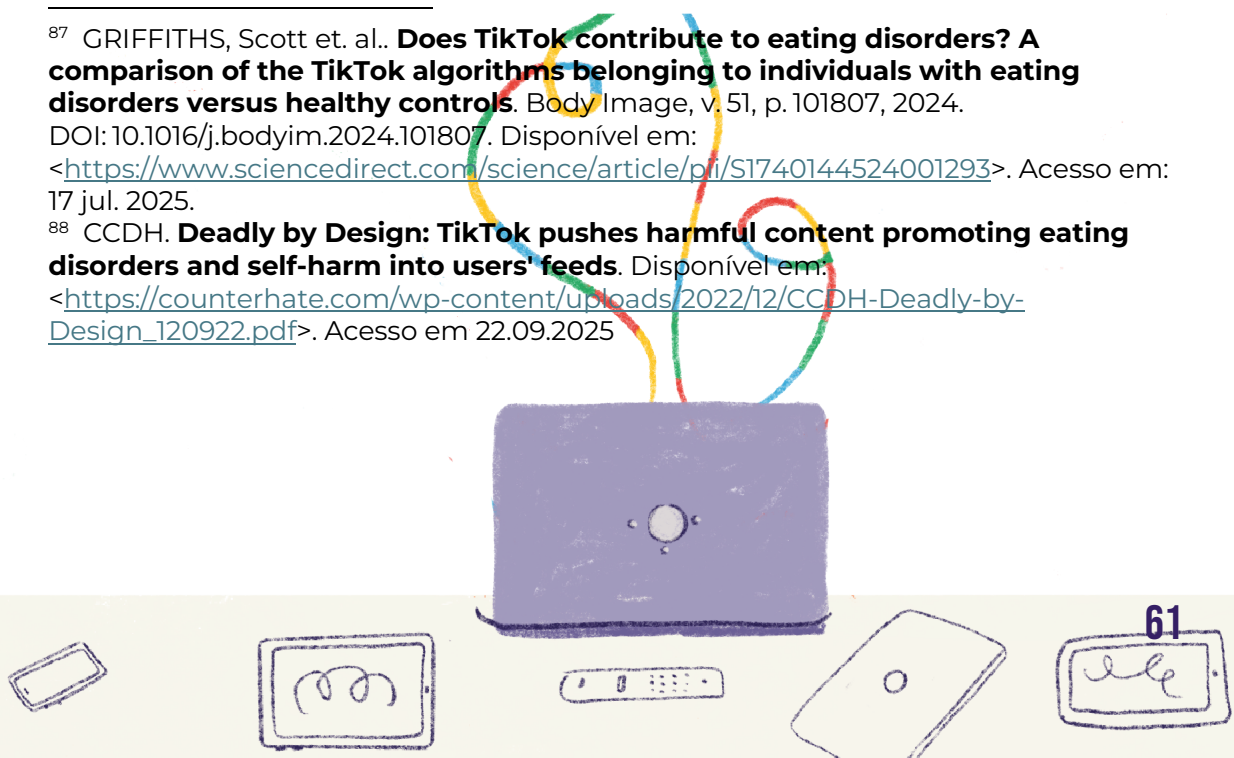
on the platform, content that is flagrantly harmful to this audience is boosted, with possible severe impacts on their lives. As an example, a study conducted by researchers at the University of Melbourne showed that TikTok's algorithmic systems recommend to users with eating disorders a 4323% higher number of videos on the topic than to other users⁸⁷. Another study, conducted by the Center for Countering Digital Hate (CCDH), showed that videos of this nature were recommended even to users under the age of 18; all they had to do was show interest in these videos for a few seconds⁸⁸.

By relying on parameters aimed at user retention, the so-called "neutrality" of personalized recommendations translates into a true free-for-all, in which inappropriate, rights-violating, and highly sensitive content is continuously offered precisely to users who can be more easily seduced by them; that is, users who already have some degree of previous vulnerability, which is then exploited by recommendation systems.

Thus, in addition to all the damage to the mental health of children and adolescents related to screen addiction, algorithmic recommendation systems informed by the logic of capturing attention at all times end up potentially aggravating preexisting mental health issues and contributing to children and adolescents who are already vulnerable to find themselves more and more surrounded by inappropriate and harmful stimuli. To face these issues, it is necessary to recognize that the promotion of different categories of harmful content usually has a common root: the additive design of social networks and the incessant battle for the attention of child users.

⁸⁷ GRIFFITHS, Scott et. al.. **Does TikTok contribute to eating disorders? A comparison of the TikTok algorithms belonging to individuals with eating disorders versus healthy controls.** Body Image, v. 51, p. 101807, 2024. DOI: 10.1016/j.bodyim.2024.101807. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S1740144524001293>>. Acesso em: 17 jul. 2025.

⁸⁸ CCDH. **Deadly by Design: TikTok pushes harmful content promoting eating disorders and self-harm into users' feeds.** Disponível em: <https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf>. Acesso em 22.09.2025



3.4.2. THE SPECIFIC IMPACTS OF ALGORITHMIC RECOMMENDATION SYSTEMS ON THE LIVES AND RIGHTS OF CHILDREN AND ADOLESCENTS

If interaction with the additive design of social networks is worthy of concern for all its users, it should be even more so when it comes to children. They are, after all, people who are going through a peculiar stage of development, marked by the still incomplete formation of the prefrontal cortex – the brain region responsible for inhibitory control, impulse control, judgment, problem solving, attention, memory, and decision-making⁸⁹. These characteristics of their stage of development make children and adolescents particularly susceptible to the development of impulsive behaviors and the formation of harmful habits, which can alter their brain structure and become practices that will accompany them for the rest of their lives⁹⁰. Not by chance, according to a survey conducted by Datafolha in September 2024, 93% of Brazilian families think that children are becoming addicted to the internet⁹¹.

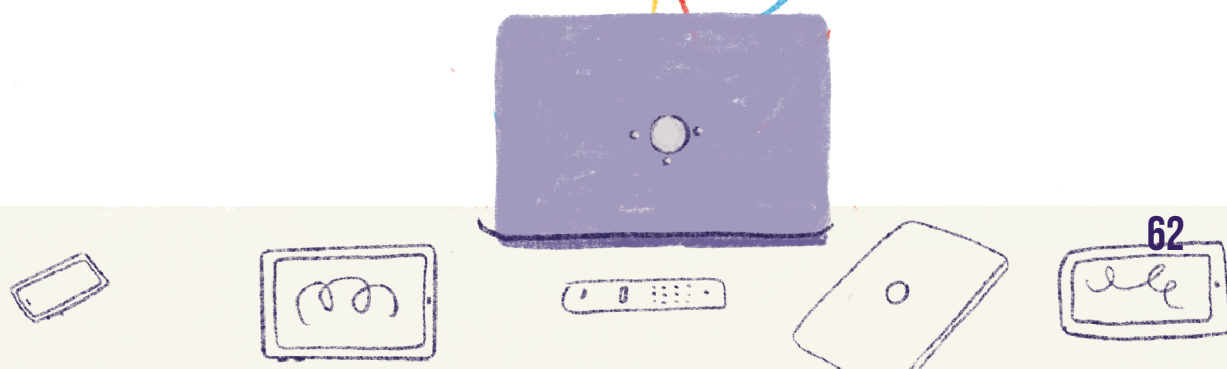
In the same vein, the compendium organized by Unicef: "The Adolescent Brain: A second window of opportunity" emphasizes that the adolescent brain is a work "in progress" and points out negative results associated with the concurrent use of multiple media streams, such as worsening memory, increased impulsivity and reduced volume in important areas of the brain, as the anterior cingulate cortex⁹². This region, specifically, is of great importance for being responsible for

⁸⁹ BRAZILIAN SOCIETY OF PEDIATRICS (SBP). **#Menos Screens #Mais Health – Update 2024**. Rio de Janeiro: SBP, 2024. Available at: <https://www.sbp.com.br/fileadmin/user_upload/24604c-MO_MenosTelas_MaisSaude-Atualizacao.pdf>. Accessed on: 17 jul. 2025.

⁹⁰ BRAZIL. Secretariat of Social Communication of the Presidency of the Republic. **Children, adolescents and screens: guide on the use of digital devices**. Brasília, 2025. p. 31. Available at: <<https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia>>. Accessed on: 14 jul. 2025.

⁹¹ CAMPOS MELLO, Patrícia. **Families think that children under 14 years old should not have a cell phone or access social media**. Folha de S.Paulo, São Paulo, 11 set. 2024. Available at: <<https://www1.folha.uol.com.br/cotidiano/2024/09/familias-acham-que-filhos-com-menos-de-14-anos-nao-devem-ter-celular-nem-acessar-rede-social.shtml>>. Accessed on: 17 jul. 2025.

⁹² UNICEF. **The Adolescent Brain: A second window of opportunity**. UNICEF Office of Research – Innocenti, 2017. 1 compendium. Florence. ISBN 978-88-6522-048-1. p.85.



controlling and managing uncomfortable emotions⁹³. As a result, it becomes more difficult to resist the urge to stay connected to networks, even if you don't want to do so.

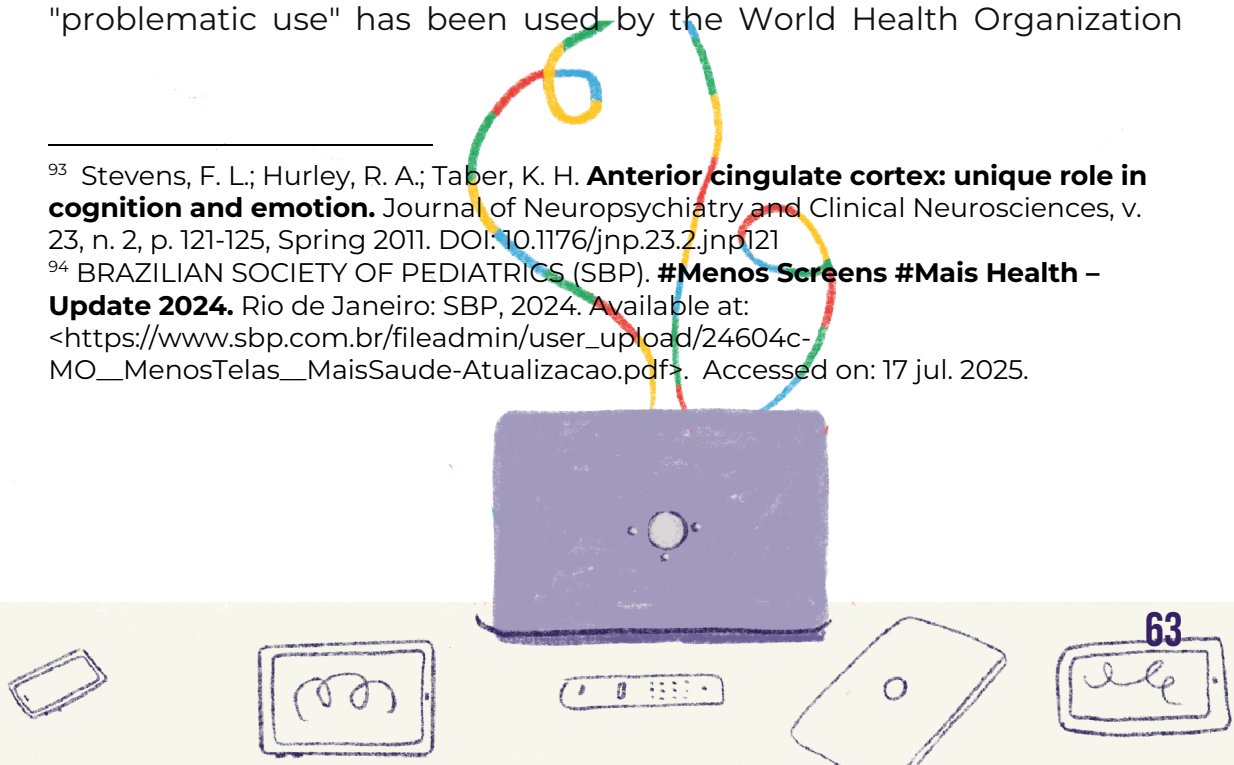
Considering that, for the business model of large technology companies, engagement equals profit, exploiting the vulnerabilities of younger people in the face of these hidden patterns becomes an advantageous practice for the commercial purposes of companies. These exploitative practices, however, directly contribute to the excessive and problematic use of digital platforms, against their own interests and, often, against their own will.

The design of social networks was thought to create variable reward cycles in users similar to those of slot machines, inducing the compulsive use of these applications to maximize the profits of the supplier companies. This use of behavioral psychology techniques to maximize user retention has as its first (and perhaps most obvious) effect the promotion of excessive and problematic use of digital technologies and the increase in time in front of screens; from which results a cascade of side effects for the development, health and well-being of children and adolescents.

The use of digital technologies is considered excessive if it exceeds the time recommended by medicine to ensure the balance of this use with other activities. In Brazil, the Brazilian Society of Pediatrics (SBP) recommends that contact with screens be zeroed for children under 2 years of age; that does not exceed 1 hour per day for children aged between 2 and 5 years; that is less than 1 or 2 hours per day for children aged between 6 and 10 years; and that it does not exceed 2 or 3 hours a day for adolescents aged between 11 and 18 years⁹⁴. The term "problematic use" has been used by the World Health Organization

⁹³ Stevens, F. L.; Hurley, R. A.; Taber, K. H. **Anterior cingulate cortex: unique role in cognition and emotion.** Journal of Neuropsychiatry and Clinical Neurosciences, v. 23, n. 2, p. 121-125, Spring 2011. DOI: 10.1176/jnp.23.2.jnp121

⁹⁴ BRAZILIAN SOCIETY OF PEDIATRICS (SBP). **#Menos Screens #Mais Health - Update 2024.** Rio de Janeiro: SBP, 2024. Available at: <https://www.sbp.com.br/fileadmin/user_upload/24604c-MO_MenosTelas_MaisSaude-Atualizacao.pdf>. Accessed on: 17 jul. 2025.



(WHO) to refer to patterns of use of technologies that take on characteristics of compulsion⁹⁵.

The incorporation of addictive design patterns and user retention techniques into the architecture of social networks works in the diametrically opposite direction to limiting the use of digital device screens for healthy or unproblematic use. In Latin America, the effects of this incorporation have been particularly sensitive: there are surveys that show that, among the 5 countries in the world with the highest average time of daily use of the internet, three of them are in Latin America: Brazil (10:08 hours a day); Colombia (10:07 hours a day) and Argentina (9:39 hours a day).⁹⁶

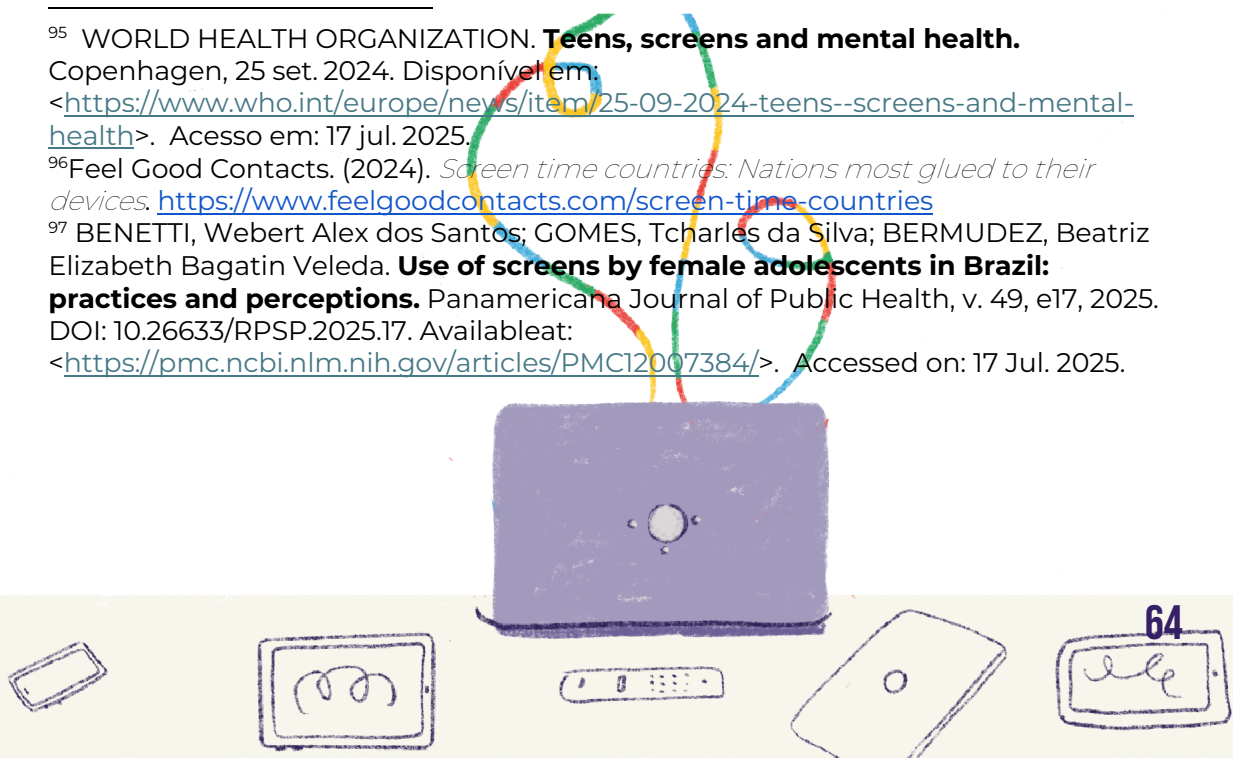
More specifically about Brazil, several pieces of evidence corroborate the perception that the dissemination of business models aimed at capturing attention has led to a scenario of excessive and problematic use of digital technologies among the younger population. A study that aimed to profile the use of screens among adolescent girls in the country reached very worrying conclusions with regard to the excessive use of screens and digital devices. Of the 214 adolescents interviewed, with a mean age of 14.9 years, 76.4% used their cell phones daily for more than 4 hours, while 25% stated that they used their cell phones for more than 9 hours every day.⁹⁷

This scenario of excessive and uncontrolled use of digital technologies, as science points out, is absolutely devastating for children and adolescents, with effects that are not even sufficiently known to accurately measure how they will be reflected and last in adult life, as this is the first generation of children and adolescents impacted by

⁹⁵ WORLD HEALTH ORGANIZATION. **Teens, screens and mental health.** Copenhagen, 25 set. 2024. Disponível em: <<https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health>>. Acesso em: 17 jul. 2025.

⁹⁶ Feel Good Contacts. (2024). *Screen time countries: Nations most glued to their devices.* <https://www.feelgoodcontacts.com/screen-time-countries>

⁹⁷ BENETTI, Weibert Alex dos Santos; GOMES, Tcharles da Silva; BERMUDEZ, Beatriz Elizabeth Bagatin Veleda. **Use of screens by female adolescents in Brazil: practices and perceptions.** Panamericana Journal of Public Health, v. 49, e17, 2025. DOI: 10.26633/RPSP.2025.17. Available at: <<https://pmc.ncbi.nlm.nih.gov/articles/PMC12007384/>>. Accessed on: 17 Jul. 2025.

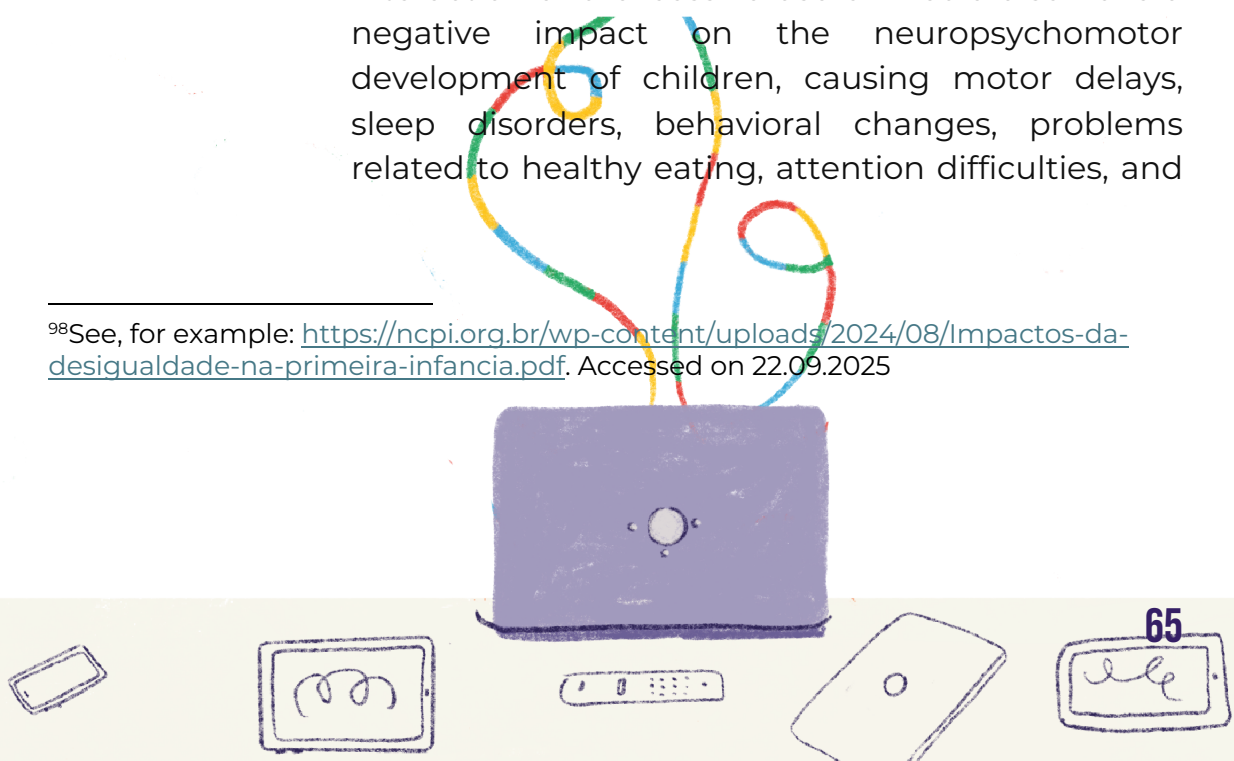


addictive design patterns. There is, however, evidence of how these effects have been materializing, which adds to the long-established knowledge about the immense impacts of childhood and adolescent experiences on people's futures⁹⁸.

Among children in early childhood, prolonged contact with screens and digital technologies has been associated with several impairments to their psychomotor and psychosocial development, including delays in speech development and cognitive development. According to a systematic survey of the pertinent literature on the subject, conducted by researchers from the Faculty of Higher Education of the Reunited Amazon (FESAR), all the articles analyzed (12/12) pointed to the existence of these losses, whose impacts are quite wide-ranging:

Intense exposure to the use of screens in early childhood, between 0 and 6 years of age, is associated with greater impairment of children's psychosocial and psychomotor development. Regarding the psychosocial consequences, social interaction disorders, damage to language domains, especially speech delay, decreased quality of affective bonds, and negative implications in the process of developing emotion regulation stand out. (...) Psychomotor consequences include limitations in activities that require fine motor skills, due to less interaction with physical toys, reduced level of physical activity, postural instability, and impairments in spatial perception, which integrates the understanding of space and movement. Early interaction and excessive use of media also have a negative impact on the neuropsychomotor development of children, causing motor delays, sleep disorders, behavioral changes, problems related to healthy eating, attention difficulties, and

⁹⁸See, for example: <https://ncpi.org.br/wp-content/uploads/2024/08/Impactos-da-desigualdade-na-primeira-infancia.pdf>. Accessed on 22.09.2025



deficits in social interaction and cognition." ⁹⁹ (free translation)

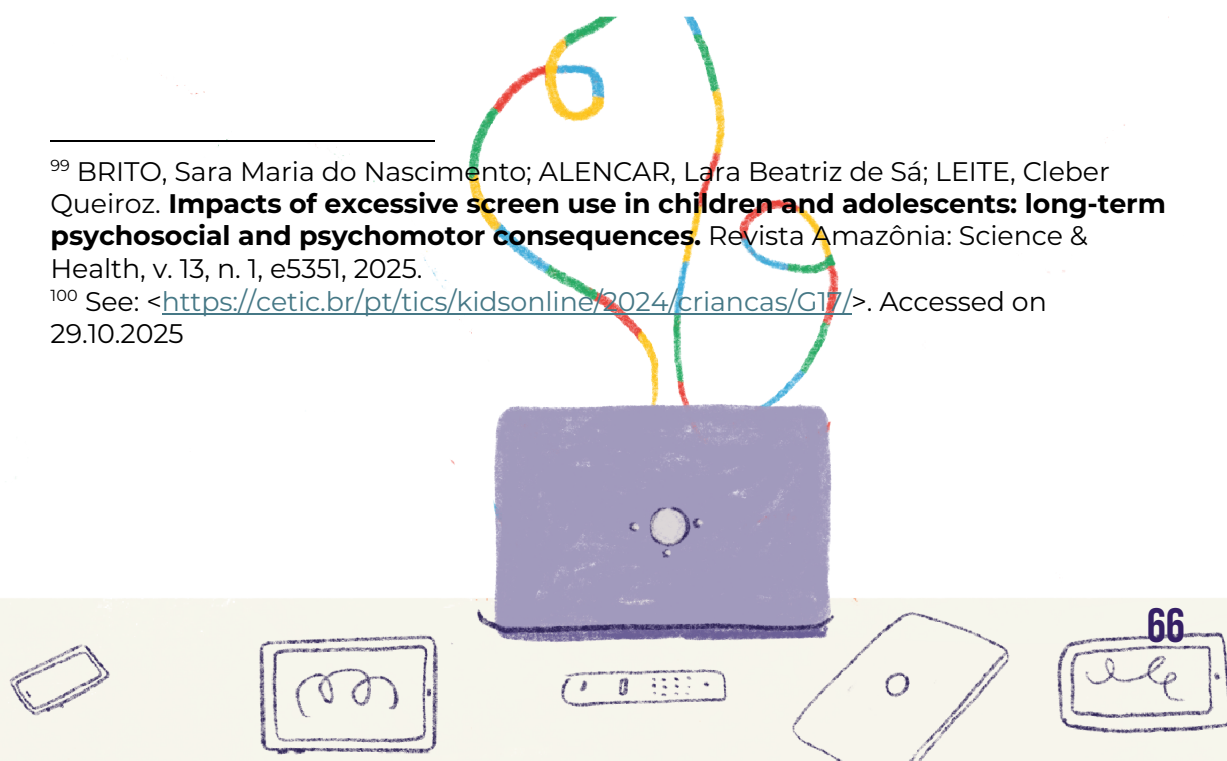
In addition to the damages listed by the study, it is worth highlighting the loss of quantity and quality of sleep as a harmful impact of addictive design. According to the SBP, sleep-related disorders are increasingly common among younger people, with harmful effects on their physical and mental health. And this does not happen by chance: according to the Tic Kids Online Brasil 2024 survey, 15% of Brazilian children and adolescents aged between 9 and 17 years old declared that they had stopped sleeping because they spent too much time on their cell phones¹⁰⁰. In the aforementioned study on the use of screens among adolescent girls, 44.2% of them stated that they prolonged the use of the cell phone until dawn.

The SBP explains that the blue light emitted by the screens of electronic devices affects the body's production of melatonin and makes it more difficult not only to fall asleep, but also to maintain a good quality of deep and restorative sleep. This leads to increased daytime sleepiness, memory problems, and reduced concentration during learning, and may be a contributing factor to the development of symptoms of attention deficit hyperactivity disorders. In addition, along with other damages caused by the excessive and problematic use of social networks, sleep loss is an element that contributes to the construction of a scenario of worsening mental health risks for children and adolescents who use applications such as TikTok.

In May 2023, the United States' top health authority, The U.S. Surgeon General's Advisory, issued an urgent public health alert about the impacts on the mental health and well-being of children and

⁹⁹ BRITO, Sara Maria do Nascimento; ALENCAR, Lara Beatriz de Sá; LEITE, Cleber Queiroz. **Impacts of excessive screen use in children and adolescents: long-term psychosocial and psychomotor consequences.** Revista Amazônia: Science & Health, v. 13, n. 1, e5351, 2025.

¹⁰⁰ See: <<https://cetic.br/pt/tics/kidsonline/2024/criancas/G17/>>. Accessed on 29.10.2025



adolescents caused by the use of social networks¹⁰¹. According to the report, young people who spend more than three hours a day on social media face twice the risk of developing mental health issues, including severe symptoms like depression and anxiety. Other mapped risks include high exposure to violent or harmful content and interactions, capable of causing damage such as decreased self-esteem, negative impacts on sleep and self-image, normalization of acts of self-inflicted harm, and suicidal ideation.

More recently, researchers at Cornell University released a study that set out to track the impacts of social media on the mental health of adolescents for 4 years. Based on this analysis, it was concluded that 31.3% of the 4285 adolescents studied had trajectories of using social networks that increasingly tended to be addictive, and that these same adolescents had a higher risk of developing suicidal behaviors compared to the others.¹⁰²

In the same vein, the report "Driven Into the Darkness: How TikTok's 'For You' Feed Encourages Self-Harm and Suicidal Ideation", by Amnesty International, shows that the harmful content recommended by TikTok's algorithmic systems further aggravates the damage generated by the platform to the mental health of children and adolescents. The reports of more than 300 children, adolescents and young people heard in the focus groups organized by Amnesty International are quite forceful in this sense, showing that the recommendation of videos guided by the logic of attention retention has very serious effects, especially for users who already have previous mental health problems:

Multiple young people with self-reported mental health concerns told Amnesty International

¹⁰¹ THE U.S. SURGEON GENERAL'S ADVISORY. **Social Media and Youth Mental Health**. 2023. Disponível em: <<https://www.hhs.gov/sites/default/files/sq-youth-mental-health-social-media-advisory.pdf>>. Acesso em 17.07.2024.

¹⁰² XIAO. Yunyu et al. **A. Addictive screen use trajectories and suicidal behaviors, suicidal ideation, and Mental Health in US Youths**. JAMA, DOI: 10.1001/jama.2025.0109. Disponível em: <<https://jamanetwork.com/journals/jama/article-abstract/2835481>>. Acesso em: 17 jul. 2025.

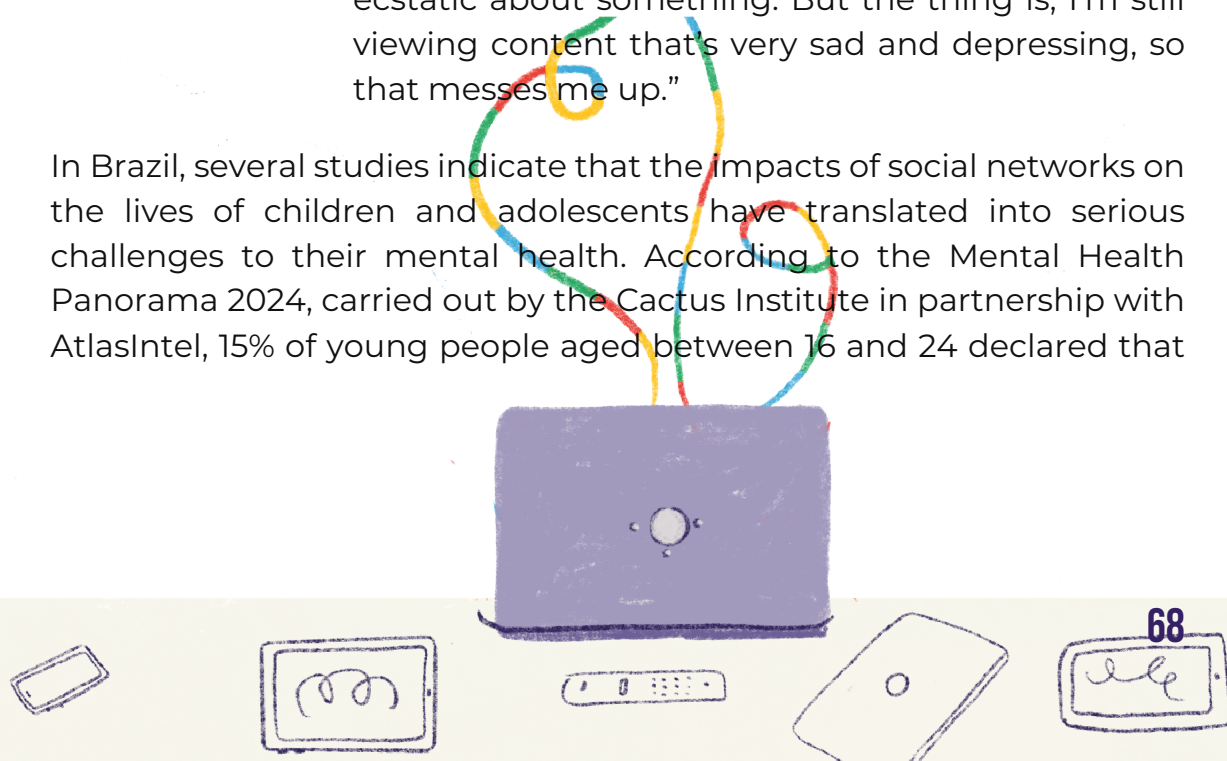


researchers about their experiences of getting drawn into TikTok's "rabbit holes" of triggering and mental health-related content. They felt that TikTok's amplification of problematic mental health-related content contributed to exacerbating their symptoms. For example, "Luis", an undergraduate student in Manila diagnosed with bipolar disorder, described his experience with TikTok's 'For You' feed: "When I felt low, I think 80% [of the content] related to mental health. It's like a spiral. It's a rabbit hole because it starts with just one video. If one video is able to catch your attention, even if you don't like it, it gets bumped to you the next time you open TikTok and because it seems familiar to you, you watch it again and then you watch it again and then the frequency of it in your feed rises exponentially."

Echoing the experience of others, "Luis" described how periods of deliberate engagement with TikTok videos reflecting his own depressive or anxious thoughts would keep him trapped in negative content loops even after the depressive phase subsided:

"TikTok assumes that you want this particular content for a particular period of time. But the thing for me is that my preferred content changes very much. For instance, one day I'm very anxious, I want this content. And one day I'm very happy and very ecstatic about something. But the thing is, I'm still viewing content that's very sad and depressing, so that messes me up."

In Brazil, several studies indicate that the impacts of social networks on the lives of children and adolescents have translated into serious challenges to their mental health. According to the Mental Health Panorama 2024, carried out by the Cactus Institute in partnership with AtlasIntel, 15% of young people aged between 16 and 24 declared that



the use of social networks had a very negative impact on their mental health, pointing to negative correlations between the loss of control over the time spent on networks and mental health indicators¹⁰³. In the previous edition of the study, it was also found that 43.5% of respondents with a diagnosis of anxiety reported spending 3 hours or more a day on social networks.

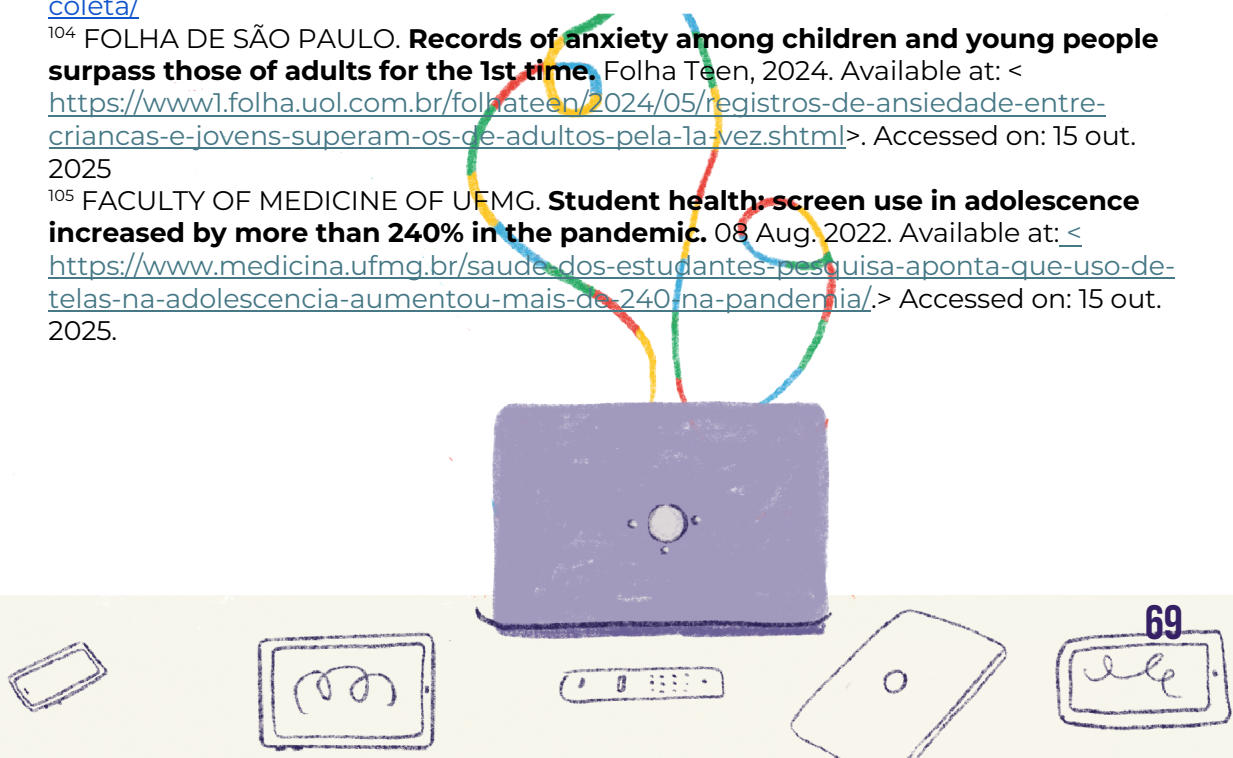
In the same direction, data related to the Psychosocial Care Network (RAPS) of the Unified Health System (SUS), consolidated by the newspaper Folha de S. Paulo, point to a large increase in records of anxiety disorders during adolescence, a phenomenon that experts relate to the cultural and behavioral changes of the last decade, such as the use of social networks¹⁰⁴. Psychiatrist Guilherme Polanczyk, from the University of São Paulo (USP), adds that the pandemic has tried to intensify an ongoing process, marked by increased exposure to social networks with addictive mechanisms and the emotional fragility of a generation still in formation.

This is exactly what can be inferred from the graph developed from the data provided by RAPS: the increase in mental health disorders among young people is visibly more pronounced from the beginning of the pandemic, coinciding with the period of intensification of the use of social networks¹⁰⁵. This correlation reinforces the warning of experts regarding the relationship between excessive consumption of content on social networks, which exploit instant reward mechanisms, and the worsening of anxiety, depression and other psychological disorders

¹⁰³Instituto Cactus. (2024, 6 de noviembre). *Panorama da Saúde Mental: 45% dos entrevistados consideram que as redes sociais afetam negativamente o bem-estar psicológico*. <https://institutocactus.org.br/panorama-da-saude-mental-terceira-coleta/>

¹⁰⁴ FOLHA DE SÃO PAULO. **Records of anxiety among children and young people surpass those of adults for the 1st time**. Folha Teen, 2024. Available at: < <https://www1.folha.uol.com.br/folha/teen/2024/05/registros-de-ansiedade-entre-criancas-e-jovens-superam-os-de-adultos-pela-1a-vez.shtml>>. Accessed on: 15 out. 2025

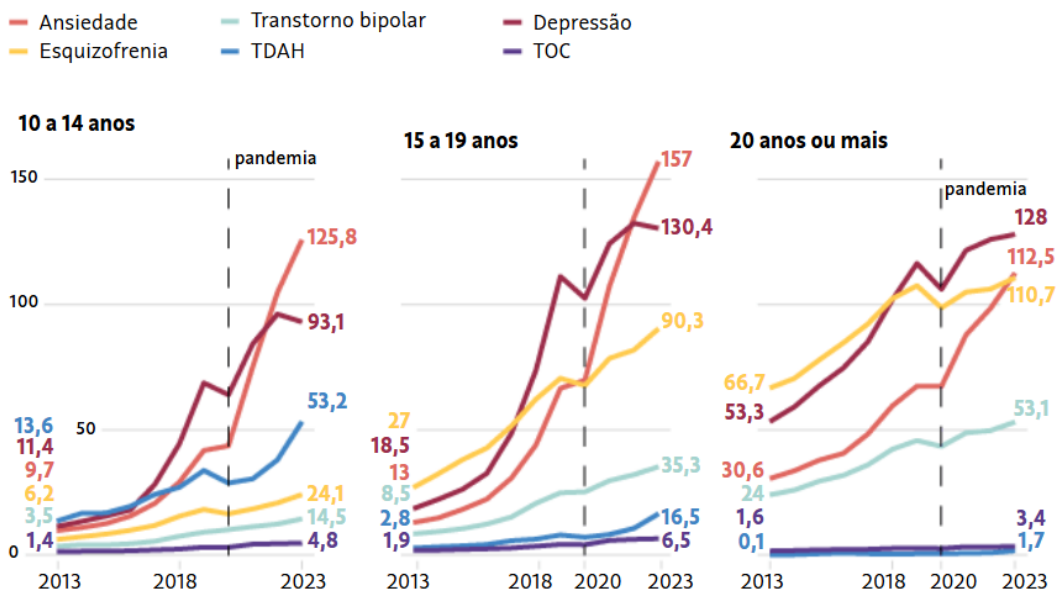
¹⁰⁵ FACULTY OF MEDICINE OF UFMG. **Student health: screen use in adolescence increased by more than 240% in the pandemic**. 08 Aug. 2022. Available at: < <https://www.medicina.ufmg.br/saude-dos-estudantes-pesquisa-aponta-que-uso-de-telas-na-adolescencia-aumentou-mais-de-240-na-pandemia/>>. Accessed on: 15 out. 2025.



among children and adolescents.

Pacientes atendidos pelo SUS, para transtornos selecionados

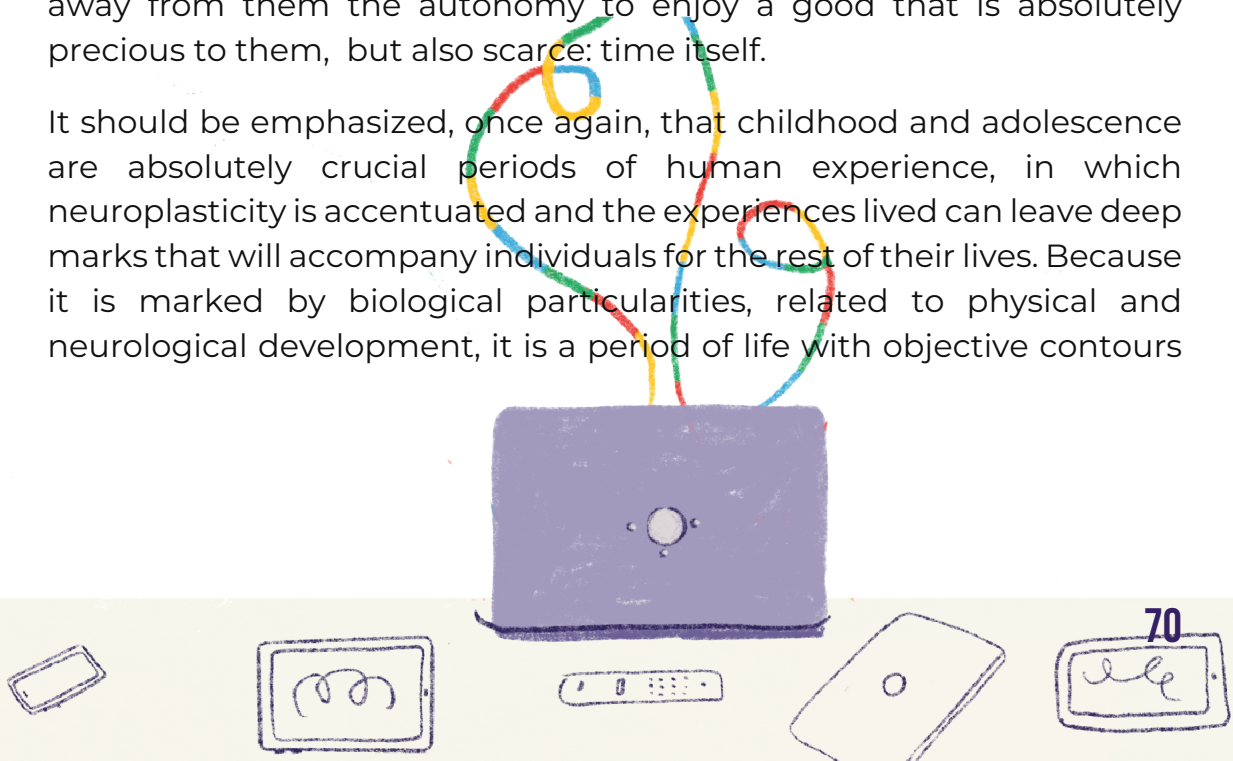
Taxa por 100 mil pessoas daquela faixa etária



Fonte: RAPS (Rede de Atenção Psicossocial) via Sistema de Informações Ambulatoriais/SUS

Although data like these are worthy of urgent attention, it is worth stressing that cases of suicide, depression and severe mental disorders represent only the most sensitive and serious part of broader losses generated by the social media business model to children and adolescents. In other words, even for those children who do not receive a diagnosis of mental health disorder, practices related to the incorporation of additive design mechanisms should be considered inappropriate, harmful and abusive, since they not only exploit the vulnerabilities of these people's developmental stage, but also take away from them the autonomy to enjoy a good that is absolutely precious to them, but also scarce: time itself.

It should be emphasized, once again, that childhood and adolescence are absolutely crucial periods of human experience, in which neuroplasticity is accentuated and the experiences lived can leave deep marks that will accompany individuals for the rest of their lives. Because it is marked by biological particularities, related to physical and neurological development, it is a period of life with objective contours

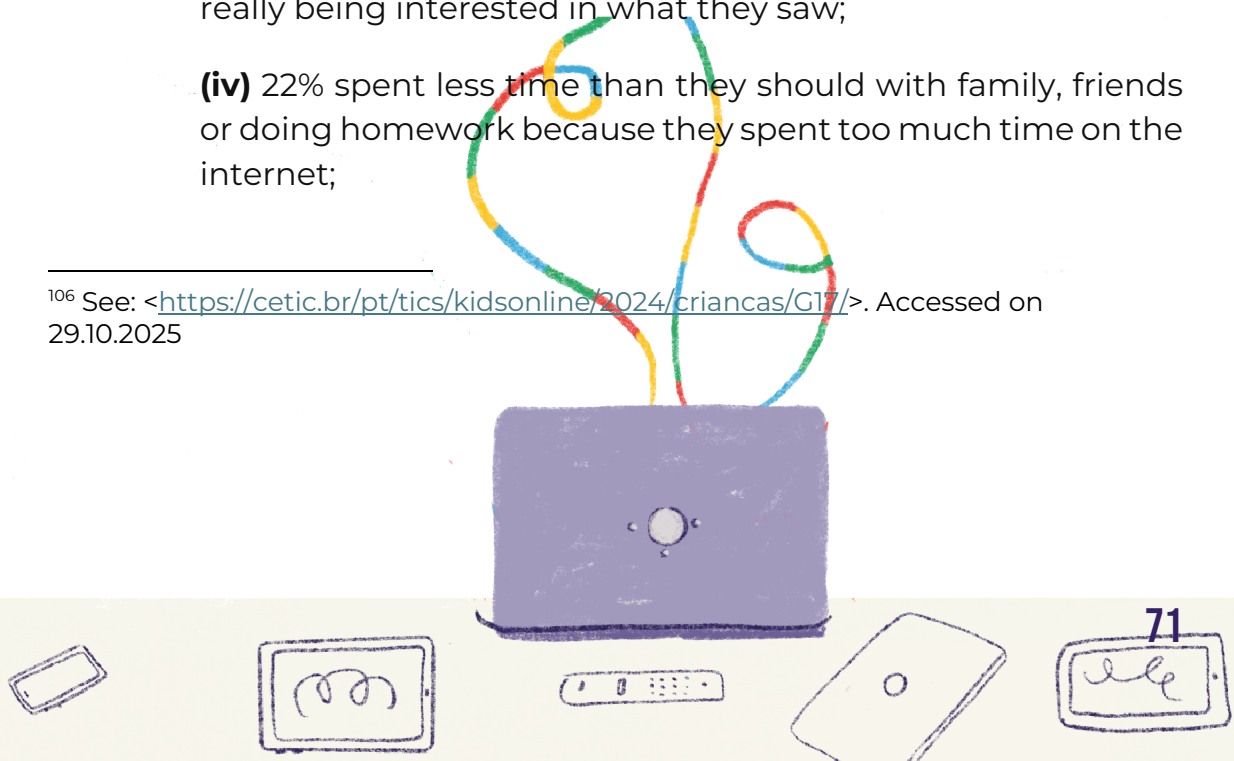


and limits: during adult life, the human brain does not have the same capacity for adaptation and absorption that it has during the first years of life; therefore, the opportunities for development and learning that one has in this period can hardly be replicated in later moments. For this reason, it is necessary to value the time of childhood and adolescence, filling it with experiences that contribute, as much as possible, to the full experience of this particular stage of human life. Children and adolescents must be given time to play freely, for affection, for contact with nature, for study, for rest and for leisure.

Analyzing the issue from this perspective, it is evident that the tactics used by social networks to addict their users and maximize their time in front of screens generate impacts that go beyond the creation of an environment conducive to the proliferation of mental health disorders and harmful content. The time spent in front of screens reduces the time available for other activities that are essential for the healthy and integral development of young people and the enjoyment of full childhoods and adolescents, and, worse, persuasive design techniques take away from children and adolescents the autonomy over the management of their time. To understand the extent of these losses, the following data collected by the 2024 edition of the Tic Kids Online Brasil survey is helpful¹⁰⁶:

- (i)** 15% of the children and adolescents interviewed stopped eating or sleeping because of the internet;
- (ii)** 16% felt bad at some point because they could not be on the internet;
- (iii)** 22% found themselves browsing the internet without really being interested in what they saw;
- (iv)** 22% spent less time than they should with family, friends or doing homework because they spent too much time on the internet;

¹⁰⁶ See: <<https://cetic.br/pt/tics/kidsonline/2024/criancas/G17/>>. Accessed on 29.10.2025



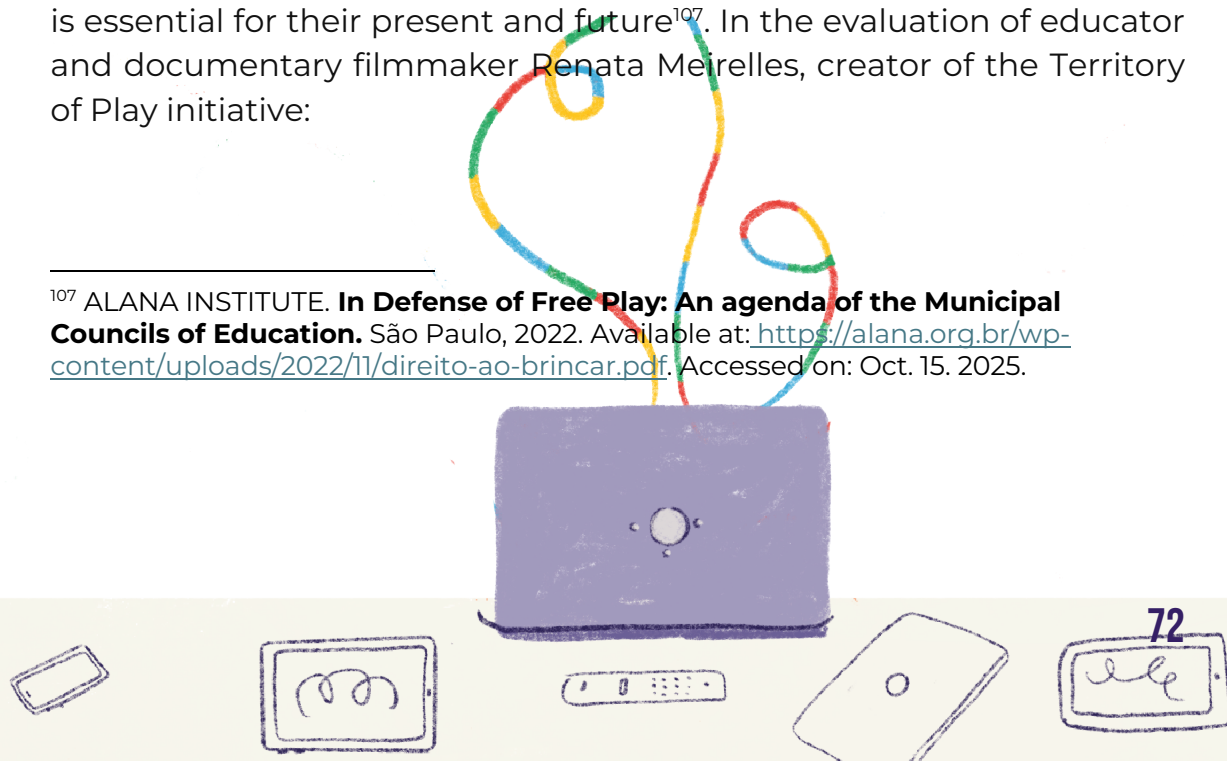
(v) 24% said they had tried to spend less time on the internet, but were unable to.

The data show that the loss of control over internet usage time already affects huge strata of the population aged between 9 and 17 years, reflecting patterns of addiction in the use of technology (problematic use) and impairments to day-to-day activities. From them, it can be extracted that the use of the internet has led to damage to other essential activities for children and adolescents, including sleep time and time with friends and family, as well as that this excessive use is taking place against the will of the younger users of digital technologies: almost 1/4 of the 4 children and adolescents interviewed said they had tried to spend less time on the internet and not succeeded, clearly revealing the scenario of loss of control over the time spent on digital platforms among children.

In this way, additive design can put in check the sleep, time for meals, body movement and social interactions of children and adolescents, in addition to one of the most crucial activities for the development of any child: play.

The act of playing freely, using the whole body, especially with other children, is of enormous importance during childhood, to the point of having been enshrined as a human and fundamental right guaranteed by Article 31 of the UN Convention on the Rights of the Child. In the early stages of life, nothing is more significant than perceiving yourself as a being who can act, move, and establish contact with others through movements and expressions. Through play, children express themselves and recognize themselves as natural, social and cultural beings, so that ensuring objective conditions for children to play freely is essential for their present and future¹⁰⁷. In the evaluation of educator and documentary filmmaker Renata Meirelles, creator of the Territory of Play initiative:

¹⁰⁷ ALANA INSTITUTE. **In Defense of Free Play: An agenda of the Municipal Councils of Education.** São Paulo, 2022. Available at: <https://alana.org.br/wp-content/uploads/2022/11/direito-ao-brincar.pdf>. Accessed on: Oct. 15. 2025.



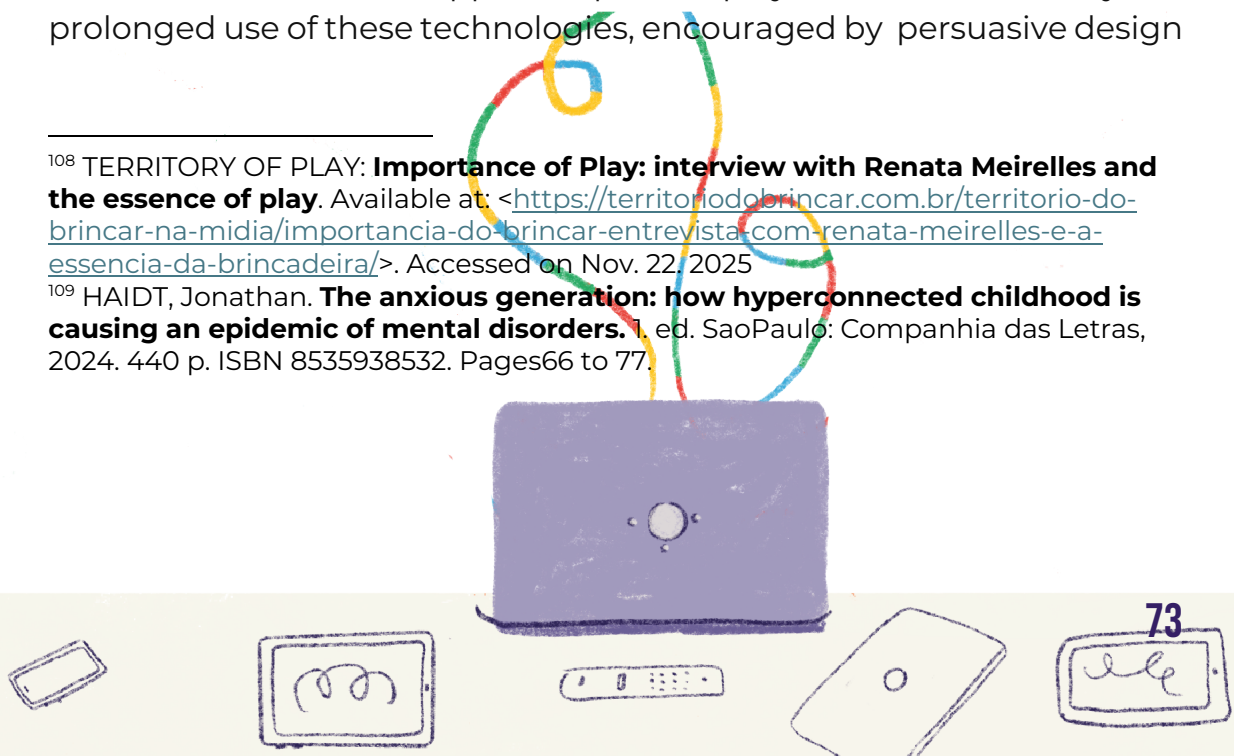
"We need to believe in the game. Believing that it itself already brings together all the necessary stimuli for children to become happy adults. There are studies that already show that adults who were children who received a lot of extra stimuli did not necessarily grow up with all the characteristics of someone fully adapted and in line with the world. But, unfortunately, we still don't believe in the power of play."¹⁰⁸

Playing is, therefore, a space and a form not only of creation but also of elaboration of who children are. It is also a space for building lasting bonds with peers and apprehending social dynamics. As Jonathan Haidt, author of "The Anxious Generation", explains, play has the role of teaching children non-verbal signals and limits for their actions, which, when incompatible with rules of coexistence already incorporated by other children, will be repressed in a low-risk environment, where making mistakes does not have significant repercussions on the socialization process¹⁰⁹s. For children, therefore, playing freely with peers is equivalent to learning, expressing and developing.

This corporeal and relational play, so essential to children's lives, however, is not experienced by them while browsing social networks. What these platforms offer, on the contrary, is a form of passive entertainment, disembodied and marked, many times, by content that is harmful to children. It is also a space where exposing oneself is equivalent to entering into a logic of self-managing, where you can be criticised at the same time by several other children or adults, resulting in an indelible loss to the needs of this moment in their lives. For Haidt, social networks are the opposite space to play. And this is also why the prolonged use of these technologies, encouraged by persuasive design

¹⁰⁸ TERRITORY OF PLAY: **Importance of Play: interview with Renata Meirelles and the essence of play.** Available at: <<https://territoriodobrincar.com.br/territorio-do-brincar-na-midia/importancia-do-brincar-entrevista-com-renata-meirelles-e-a-essencia-da-brincadeira/>>. Accessed on Nov. 22, 2025

¹⁰⁹ HAIDT, Jonathan. **The anxious generation: how hyperconnected childhood is causing an epidemic of mental disorders.** 1. ed. Sao Paulo: Companhia das Letras, 2024. 440 p. ISBN 8535938532. Pages 66 to 77.



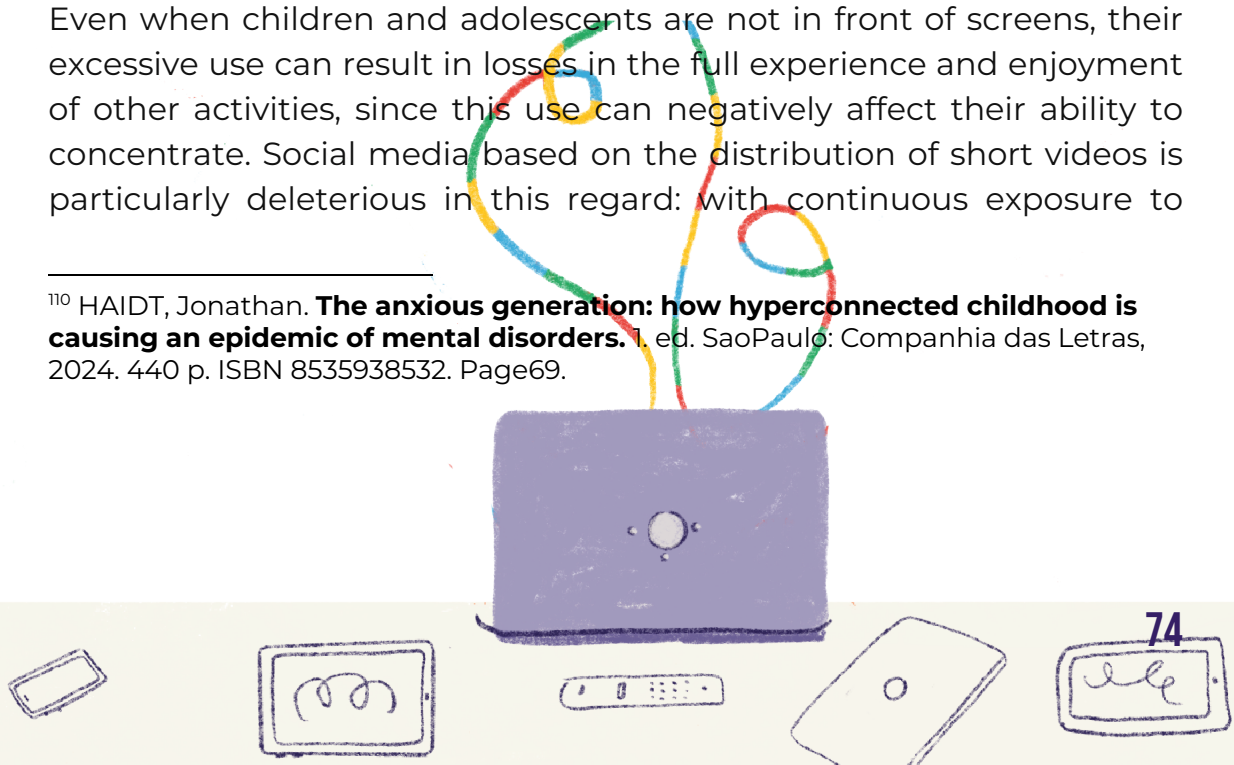
techniques, deprives children of activities that are essential to them. In Haidt's words:

"While the content of these sites could be filtered to remove harmful material, the addictive design of these platforms reduces the time available for face-to-face play in the real world, to the point that we can refer to smartphones and tablets as inhibitors of experiences in the hands of children. Of course, a smartphone opens up worlds of new experiences, including online games (which are a form of play) and long-distance relationships. However, the cost of this is the reduction of the kind of experience that humans have evolved to have and that they need in abundance to become socially functioning adults. It's as if we handed our kids iPads full of movies about walking, but the movies were so engaging that the kids never put in the time or effort necessary to actually walk."¹¹⁰

Haidt's reflections dialogue with the multiple losses mapped by the literature related to the decrease in interpersonal interactions caused by excessive screen time. The social interaction disorders, damage to language domains, especially speech delay, decreased quality of affective bonds, and negative implications in the process of developing emotion regulation, highlighted by the literature review study mentioned in this topic, are directly related to this deprivation of social interaction in the first years of life, since they are related to skills that cannot be learned without direct contact with other people.

Even when children and adolescents are not in front of screens, their excessive use can result in losses in the full experience and enjoyment of other activities, since this use can negatively affect their ability to concentrate. Social media based on the distribution of short videos is particularly deleterious in this regard: with continuous exposure to

¹¹⁰ HAIDT, Jonathan. **The anxious generation: how hyperconnected childhood is causing an epidemic of mental disorders**. 1. ed. Sao Paulo: Companhia das Letras, 2024. 440 p. ISBN 8535938532. Page 69.



these videos, the brains of platform users become accustomed to rapid and successive stimuli, gradually becoming less able to absorb denser information or to keep their attention on the same thing for longer periods of time. Therefore, several studies have shown negative correlations between the consumption of short videos and motivation and academic performance^{111 112 113}.

The loss of the ability to maintain attention for long periods of time has severe implications for several spheres of the lives of children and adolescents, in addition to education. The ability to concentrate is instrumental for planning, long-term problem solving and the possibility of reflection and development of critical thinking about the information with which one has contact. It is also an essential condition for experiences to be lived in their fullness, with presence and significance. When this capacity is undermined, experiences tend to become more superficial and the possibilities of agency over the world and what is apprehended from it are reduced. "Life becomes something smaller than it could be," in the words of writer and activist Johann Hari.¹¹⁴

The question that arises here, therefore, goes beyond the protection of the mental health of children and adolescents: what is at stake is the preservation of the time of childhood and adolescence, so that children and adolescents can enjoy this stage of their lives freely, doing activities that will contribute to their well-being and integral development, and

¹¹¹ LIAO, Mingyue. **Analysis of the causes, psychological mechanisms, and consequences of social network addiction in China**. Frontiers in Psychology. 6 ago. 2024. Disponível em:

<<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11333346/>>/. Acesso em: 14 jul. 2025.)

¹¹² XIE, Jin, et al. **The effect of short-form video addiction on undergraduates' academic procrastination: a moderated mediation model**. Frontiers in Psychology, Lausanne, v. 14, art. 1298361, 15 dez. 2023. DOI: 10.3389/fpsyg.2023.1298361. Disponível em: <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10756502/>>/. Acesso em: 17 jul. 2025.

¹¹³ YE, Jian Hong et al. **Effects of short video addiction on the motivation and wellbeing of Chinese vocational college students**. Frontiers in Public Health, Lausanne, v. 10, art. 847672, 09 maio 2022. DOI: 10.3389/fpubh.2022.847672. Disponível em: <<https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2022.847672/full>> cesso em: 17 jul. 2025.

¹¹⁴ HARI, Johann. **Stolen Focus: Why can't you pay attention**. Translated to portuguese by Luis Reyes Gil. Page 21. 1. ed. Porto Alegre: Vestigio, 2023. 320 p. ISBN 978-6560020047.



not seeing themselves captured by addictive mechanisms of attention retention that, in an insidious way, not only reduce the availability of time for other activities, but also make these people's time less profitable even when they are not in direct contact with screens. Some organizations already estimate that today's children and adolescents will spend 25 years of their lives scrolling on their cell phones.¹¹⁵ This must be read, in itself, as an inestimable damage and a serious violation of their rights, to be analyzed in the light of the child protection norms in force in International Law.

¹¹⁵ SCRIPPS NEWS. **Students on track to spend 25 years of their lifetime on phones, study warns.** Disponível em: <<https://www.scrippsnews.com/science-and-tech/social-media/students-on-track-to-spend-25-years-of-their-lifetime-on-phones-study-warns>>. Acesso em: 18 jul. 2025.

