

doi <https://doi.org/10.5020/2317-2150.2026.17323>

Algorithmic determinism, consumer freedom of choice, and heightened vulnerability *Determinismo algorítmico e direito de escolha do consumidor e o agravamento de sua vulnerabilidade*

Determinismo algorítmico y derecho de elección del consumidor: el agravamiento de su vulnerabilidad

Cláudio José Franzolin* <https://orcid.org/0000-0002-9594-1238>, Pontifical Catholic University of Campinas, Campinas, São Paulo, Brazil.

Maria Clara Giasseti Medeiros Corradini Lopes** <https://orcid.org/0009-0007-6333-8956>, Pontifical Catholic University of Campinas, Campinas, São Paulo, Brazil.

Editorial

Article History

Received: 03/09/2026

Accepted: 06/22/2026

Thematic Axis 3 – Law, Technology, and
a Changing Society

Editores-chefes

Katherinne de Macêdo Maciel Mihaliuc
Universidade de Fortaleza, Fortaleza, Ceará,
Brasil
katherinne@unifor.br

Sidney Soares Filho

Universidade de Fortaleza, Fortaleza, Ceará,
Brasil
sidney@unifor.br

Editor Responsável

Sidney Soares Filho
Universidade de Fortaleza, Fortaleza, Ceará,
Brasil
sidney@unifor.br

Author

Cláudio José Franzolin
cfranzol30@gmail.com
Contribution: content inclusion,
text review and supervision.

Maria Clara Giasseti Medeiros
mariagiasseti@gmail.com
Contribution: initial drafting,
conception, methodology, data collection.

How to cite:

FRANZOLIN, Cláudio José; LOPES, Maria Clara Giasseti
Medeiros Corradini. Algorithmic determinism,
consumer freedom of choice, and heightened
vulnerability. *Pensar – Journal of Legal Sciences*,
Fortaleza, v. 31, e17323, 2026. DOI: <https://doi.org/10.5020/2317-2150.2026.17323>

Data Availability Statement

Pensar – Journal of Legal Sciences adopts Open
Science practices and makes available, alongside this
publication, the Data Availability Statement (Pensar
Data Form) completed and signed by the authors.
The document contains information regarding the
nature of the article and the possible existence of
supplementary data. It is available as a supplementary
file on the journal's website.

Abstract

This study investigates the impact of artificial intelligence used by suppliers on consumers' fundamental right to choose in the digital marketplace. The central problem lies in algorithmic determinism, which uses the processing of massive datasets to predict behavior and restrict decision-making autonomy, transforming freedom of choice into an "illusory freedom." The general objective is to analyze the exacerbation of structural digital vulnerability and the need for public policies and ex ante regulatory governance to protect consumers' right to choose. Methodologically, the study adopted a qualitative, exploratory, and descriptive approach based on bibliographic and documentary research and analytical reasoning. The findings demonstrate that tools such as profiling, nudges, and dark patterns promote "algorithmic colonization," resulting in discriminatory practices such as the pink tax and geoprizing. These mechanisms reduce consumers to mere informational assets, exacerbating their hypervulnerability. The article concludes that the current reactive legal system is insufficient and proposes a systematic interpretation of the Brazilian Consumer Protection Code in conjunction with the Brazilian General Data Protection Law (LGPD). The study's main contribution is its defense of transparency and the right to an explanation under Article 20 of the LGPD as essential mechanisms for safeguarding human dignity and decision-making autonomy in the face of surveillance capitalism.

Keywords: algorithmic determinism; digital vulnerability; consumer law.

Resumo

O presente estudo investiga o impacto da Inteligência Artificial (IA) manejada por fornecedores sobre o direito básico de escolha do consumidor no mercado digital. O problema central reside no determinismo algorítmico, que utiliza o processamento de dados massivos para prever comportamentos e restringir a autonomia decisória, transformando a liberdade de escolha em uma "liberdade fictícia". O objetivo geral é analisar o agravamento da vulnerabilidade digital estrutural e a necessidade de políticas públicas e de governança regulatória ex ante para proteger o direito de escolha do consumidor. Metodologicamente, adotou-se uma abordagem qualitativa, exploratória e descritiva, fundamentada em pesquisa bibliográfica e documental, com método de raciocínio analítico. Os resultados demonstram que ferramentas como profiling, nudges e dark patterns promovem uma "colonização algorítmica", resultando em práticas discriminatórias como a Pink Tax e o geoprizing. Tais mecanismos convertem o consumidor em um mero ativo informacional, agravando sua hipervulnerabilidade. O artigo conclui que o sistema jurídico reativo atual é insuficiente, propondo uma interpretação sistemática entre o Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de Dados Pessoais (LGPD). A principal contribuição do estudo é a defesa da transparência e do direito à explicação (artigo 20 da LGPD) como ferramentas essenciais para garantir a dignidade humana e a soberania decisória frente ao capitalismo de vigilância.

Palavras-chave: determinismo algorítmico; vulnerabilidade digital; direito do consumidor.

Resumen

El presente estudio investiga el impacto de la Inteligencia Artificial (IA) utilizada por los proveedores sobre el derecho básico de elección del consumidor en el mercado digital. El problema central radica en el determinismo algorítmico, que emplea el procesamiento masivo de datos para predecir comportamientos y restringir la autonomía decisoria, transformando la libertad de elección en una "libertad ficticia". El objetivo general consiste en analizar el agravamiento de la vulnerabilidad digital estructural y la necesidad de políticas públicas y de gobernanza regulatoria ex ante para proteger el derecho de elección del consumidor. Metodológicamente, se adoptó un enfoque cualitativo, exploratorio y descriptivo, fundamentado en investigación bibliográfica y documental, con método de razonamiento analítico. Los resultados demuestran que herramientas como el profiling, los nudges

* Master's and PhD in Law. Professor and Researcher, full-time dedication, at School of Law of PUC-Campinas.

** Master's in Human Rights and Social Development from PUC-Campinas, specialist in Constitutional Law and Digital Law. Coordinator of Law and Technology at National Institute for Human Rights Research and Promotion.



y los darkpatterns promueven una «colonización algorítmica», dando lugar a prácticas discriminatorias como la Pink Tax y el geoprising. Tales mecanismos convierten al consumidor en un mero activo informacional, agravando su hipervulnerabilidad. El artículo concluye que el sistema jurídico reactivo actual resulta insuficiente y propone una interpretación sistemática entre el Código de Defensa del Consumidor (CDC) y la Ley General de Protección de Datos Personales (LGPD). La principal contribución del estudio consiste en defender la transparencia y el derecho a la explicación (artículo 20 de la LGPD) como herramientas esenciales para garantizar la dignidad humana y la soberanía decisoria frente al capitalismo de vigilancia.

Palabras clave: determinismo algorítmico; vulnerabilidad digital; derecho del consumidor.

1 Introduction

The exponential advancement of technology and the widespread use of artificial intelligence (AI) have revolutionized social relations and notably transformed the consumer landscape, culminating in the rise of platform capitalism and the digital marketplace. In this context, companies make extensive use of AI to personalize their interactions with consumers and optimize the provision of products and services. However, this digital expansion has also ushered in uncertain times for consumer protection, as discriminatory practices and technological mechanisms that covertly interfere with consumer choices through algorithms have become increasingly prevalent.

The core of the challenge lies in the fact that sophisticated algorithms and consumer profiling allow suppliers to subtly and invisibly monitor and influence user behavior. In this context, decision-making is taken away from individuals through the collection of their browsing histories and online searches – i.e., their “micro-behaviors” on digital networks. This manipulation erodes consumers’ decision-making rationality, autonomy, and freedom. The question therefore arises: where is the boundary between beneficial and harmful forms of influence?

Consider, for example, the following scenario: a consumer routinely selects a particular music genre on a streaming platform. Based on these choices, AI begins suggesting a vast array of performers and bands in the same genre and style with which the consumer has never previously engaged or listened to.

In such a situation, could it be argued that the supplier, by operating the platform through AI, is inducing the consumer to engage with these new performers and bands? Would this be detrimental to the consumer? Conversely, might the consumer view the platform’s recommendations positively because they facilitate exposure to new performers or bands? The question remains: to what extent may a supplier use algorithms to influence consumers who use its platform? Does this practice affect consumers’ fundamental right to choose? This is the new reality of consumer relations: it is more digital and sophisticated and has the capacity to know consumers’ preferences better than consumers themselves do. Is this the direction in which consumer society is headed?

According to Comitê Gestor da Internet no Brasil (2025, p. 85), more than 70% of the population made purchases online. The survey results also indicate that 71% of Brazilian households with internet access connected through fixed broadband, including 65% through fiber-optic connections, while 14% relied on mobile connections. Another survey found that, in 2024, 92% of internet users sent instant messages, 82% made voice or video calls, and 81% used social media. Moreover, according to the survey, six out of ten internet users aged ten or older searched for information about products or services (56%).

Along the same lines, the report prepared by Comitê Gestor da Internet no Brasil (2025) found that 46% of users purchased products or services online, corresponding to approximately 73 million people. The most frequently sought and purchased products were clothing, footwear, and sporting goods (71%), followed by household appliances (53%), food or food products (45%), and cosmetics or personal hygiene products (41%). The most sought-after services included ride-hailing applications used to request taxis and private drivers (44%), online movie and television series streaming services (40%), and meal delivery services (35%).

This reality enables suppliers to collect consumers’ personal data, which have become valuable assets in business operations.

Suppliers are increasingly operating across national borders despite having no legal or commercial presence in the country, particularly in the context of marketplaces and dropshipping. This reality has now acquired a new dimension: AI.

In this context, the Comitê Gestor da Internet states that AI on the internet “requires substantial connectivity capacity.” Comitê Gestor further warns that “the Brazilian population may become consumers of AI-generated content without having access to the practical use of AI and without being able to distinguish the reality produced by AI”¹ (Comitê Gestor da Internet, 2025, p. 95).

¹ For the purposes of this article, all direct quotations from the original sources have been translated into English.

Supporting this assertion, data from the Capgemini Research Institute (2025) indicate that 64% of consumers are willing to purchase new products or services recommended by AI. This percentage rises to 74% among younger consumers who live with family members, relatives, or guardians.

Compared with other countries worldwide, Brazil ranks second globally in consumers' daily interactions with AI. This finding indicates that people in Brazil are extensively exposed to intelligent agents, often without realizing that they are not interacting with human beings.

As economy becomes increasingly platformized (Carvalho; Franco Neto; Verbicaro, 2024, p. 154), AI incorporates disruptive technologies and telecommunications systems operated by suppliers, providing them with extensive information. Through the large-scale collection of consumers' personal data, suppliers can employ predictive techniques to anticipate user behavior. In other words, this dematerialized, instantaneous reality has become so sophisticated that suppliers can assess, analyze, and understand consumers better than consumers understand themselves.

This means that consumers' right to choose is undermined to the point that they become trapped within their own browsing patterns, which are shaped as they navigate the internet.

In light of these emerging technologies, this study investigates consumer protection and the need to strengthen it, particularly because these technologies enable consumers to be selected and categorized, thereby compromising their right to choose (Agrassar, 2025).

This study addresses three interconnected issues: i) suppliers' use of algorithms; ii) the platformization of the economy; and iii) the importance of public policies for protecting consumers, who are expressly recognized as vulnerable (Brasil, 1990). This perspective underpins the theoretical premise discussed herein: algorithmic determinism.

Our research question is as follows: How do algorithmic determinism and the opacity of AI tools used by suppliers compromise consumers' fundamental right to choose, and how can ex ante regulatory governance mitigate the exacerbation of this vulnerability in the digital environment?

The general objective of this study is to recognize the heightened vulnerability of consumers – which has evolved into structural or algorithmic digital vulnerability – in the digital marketplace and to analyze the need for public policies and regulatory governance to protect consumers' right to choose, particularly in view of its collective dimension (Article 2, sole paragraph, of Law No. 8,078/1990).

The specific objectives are to conceptually delineate algorithmic determinism; identify data-collection and manipulation practices, such as dark patterns, that exacerbate consumer vulnerability; and explain the challenges involved in assessing the explainability of automated decisions.

As a technical procedure, the investigation was structured as bibliographic and documentary research. The methodological process began with a critical review of specialized Brazilian and international literature, focusing on digital advertising, algorithmic vulnerability, profiling, and the control strategies used by suppliers. In addition, the documentary research encompassed an analysis of technical reports and empirical market data demonstrating the use of products and services designed to shape consumer behavior.

This study also adopts a qualitative, exploratory, and descriptive approach. It employs analytical reasoning, beginning with a conceptual and macrosocial analysis of algorithmic determinism and platform capitalism. It then uses data drawn from reports to examine the products and services most frequently used by suppliers to influence consumer choices, as well as the economic implications of such practices.

Accordingly, the research process is grounded in a critical review of the literature, particularly studies addressing digital advertising, data vulnerability, profiling, and suppliers' use of algorithmic determinism.

This methodological framework was selected because of the need to develop an in-depth understanding of the central elements of AI in consumer relations and to assess its direct effects on consumers' freedom of decision-making and individuality. Ultimately, the investigation sought to correlate the legal doctrine of consumer vulnerability (Brasil, 1990, Article 4, item I) with the sociopolitical implications of algorithmic colonization in order to propose a new ethical model grounded in transparency and ex ante regulatory governance.

The authors declare that AI was not used to produce the text or as a research source. Its use was limited to the linguistic refinement of specific paragraphs to improve the clarity and concision of the writing, including paragraph restructuring and the selection of more appropriate terminology.

NotebookLM, an AI tool, was used during the final review of the article to identify grammatical or typographical errors and to verify the correspondence between the works cited in the body of the study and the final reference list². However, the review of the text did not rely exclusively on this technology.

² The prompts used were: "Help me proofread the paper for grammatical errors"; "List all agreement and typographical errors in the text"; "Check whether all citations in the body of the text are included in the reference list"; and "Check whether the references are listed in alphabetical order, consistently formatted, and compliant with ABNT standards."

In conclusion, this research is warranted by the increasing digitalization of consumer relations in Brazil. In addition to more than 80% of connected Brazilian consumers making purchases online, Brazil ranks second globally in interactions with AI. The sophistication of these technologies allows suppliers to know consumers better than consumers know themselves, creating a landscape of algorithmic colonization and discrimination, including practices such as geopricing and the pink tax, that the current reactive legal framework cannot fully address.

2 Digital consumption and the threat to autonomy in the age of algorithms

The onset of the COVID-19 pandemic and the resulting mandatory isolation of the population intensified suppliers' use of increasingly complex digital tools (Domingues, 2021).

This scenario calls for an in-depth examination of how extensive digitalization, when structured by suppliers in abusive or harmful ways, affects individual autonomy and consumers' right to choose. This section therefore analyzes the impact of digital consumption and the growing influence of algorithms on individual freedom of decision-making, exploring the mechanisms of control and personalization that shape online behavior and, consequently, autonomy in the digital age.

2.1 Algorithmic determinism and AI

The core of the problem lies in the opacity of these technologies, which affects how consumers choose products or services (Agrassar, 2025). It is therefore essential to understand algorithmic determinism.

AI is defined as the "set of instructions that enables machines to perform tasks characteristic of human intelligence, such as planning, language comprehension, and learning" (Pereira; Teixeira, 2019, p. 119-142).³

In short, AI systems are trained on massive datasets, or big data, that are processed by algorithms. In its fragmented form, data constitute raw material that, once organized and mediated through machine learning, is transformed into information and subsequently into predictive knowledge (Verbicaro; Moura, 2025).

From this perspective, algorithmic determinism concerns the processing capacity of this technology, which is used to construct and select behavioral patterns from data in ways that may affect consumers' fundamental rights.

The question arising from this context is: To what extent is this beneficial or harmful to consumers? Algorithmic determinism emerges within this context of choices directed toward consumers.

Algorithmic determinism should not be understood merely as an external influence but as a structure grounded in technical control that anticipates the choices consumers might make based on their profiles, digital footprints, online browsing activities, and collected data. This determinism represents the means by which suppliers dictate consumer behavior, based on the premise that algorithms will always produce the same output from the same input (Verbicaro, 2023). Verbicaro (2023) discusses the use of algorithms before consumers make decisions, thereby predicting and influencing future decisions (Verbicaro; Moura, 2025). In other words, the aim is to predetermine an individual's future, undermining decision-making autonomy and imposing standardized patterns (Spagnollo; Tonial, 2023).

Algorithms interpret consumer behavior recursively; that is, they rely on users' own browsing habits to recalibrate targeting with greater precision. Following this reasoning, new recommendations presented to consumers may be recalibrated based on the activities monitored by AI (Abrusio, 2020). In other words, internet browsing, which consumers once conducted freely, has now become a structured, controlled, and monitored activity.

In this context, the right to personal data protection and consumers' right to choose are compromised. This situation further exacerbates consumer vulnerability, giving rise to what Marques and Mucelin (2022, p. 1) describe as "structural digital vulnerability."

Thus, when suppliers interfere with consumer consent and choice, three foundations of the Brazilian General Data Protection Law (LGPD) (Brazil, 2018) are disregarded: informational self-determination, the fundamental rights established in the Brazilian Consumer Protection Code (CDC) (Brazil, 1990), and human rights.

The argument advanced here concerns the seriousness of algorithmic modulation in light of its potentially harmful effects on society. After all, if an algorithm predicts consumers' futures in a deterministic manner and treats them based on those predictions, consumers do not possess genuine freedom of choice or the ability to act more freely (Agrassar, 2025). This situation consequently calls into question the interface between law and algorithms.

³ For the purposes of this article, all direct quotations from the original sources have been translated into English.

While the law operates through concepts such as justice, equity, and reasonableness, algorithms operate through binary logic and outcome optimization. Given this disconnect, consumer protection assumes particular importance under the LGPD through the right to an explanation, as discussed by Frazão and Goettenauer (2020). However, a legal analysis of algorithmic determinism cannot rely solely on ex post regulation through compensation for harm; it requires ex ante governance.

In summary, by transforming human experience into predictive behavioral data (Zuboff, 2020), algorithmic determinism driven by AI challenges the protection of the right to information and consumers' right to choose.

2.2 Profiling, consumers' illusory freedom, and the interface with artificial intelligence

The development of AI is intrinsically related to the capacity to collect, process, and monetize what is known as behavioral surplus.

In this regard, Zuboff (2020) explains that behavioral surplus, which underpins the wealth of search platforms such as Google, consists of surveillance assets – i.e., essential raw materials for generating revenue.

Algorithmic profiling emerges within this context and consists of analyzing consumers and constructing a “prototype” of them. This mechanism seeks to map every aspect of users' lives – including workplace behavior, personal lives, consumption habits, and locations – as they interact with digital networks and platforms. Profiling may also result in discriminatory strategies based on algorithms' evaluations of users' searches. Technology may thus be used to reject certain consumer profiles because it attempts to determine consumers' routines, browsing and purchasing habits, and movements based on their searches (Carvalho; Franco Neto; Verbicaro, 2024).

Data collection is often invisible and subtle because it occurs through cookies installed on users' computers, allowing their preferences to be tracked. It also allows searches and content to be directed according to the preferences and habits users develop in digital environments. By using cookies to collect consumers' browsing and purchasing habits, suppliers can infer choices and characteristics related to religion, sports, sexuality, politics, and health, including chronic health conditions. By consenting to the collection of their preferences, users exacerbate their own vulnerability (Guimarães, 2023).

Consumers have no meaningful alternative: they must either accept the terms and conditions to access a digital platform or service or refuse them and forgo access – the “take it or leave it” model. This reality creates “involuntary” or merely apparent consent (Chaves, 2025, p. 17836), compromising consumers' genuine, free, and uncoerced consent, as well as their informational self-determination (Marques; Mucelin, 2022).

Digital platforms use AI as part of their preference-collection strategies to influence consumer behavior, often invisibly (Carvalho; Franco Neto; Verbicaro, 2024). Human decisions are therefore subject to increasingly extensive analysis (Agrassar, 2025).

According to Domingues (2021, p. 2), algorithms collect personal information and use it to make decisions that are more objective than human decisions. From the perspective of economic rationality, Kahneman (2021) argues that human decisions are not optimal because they are influenced by how choices are framed.

In other words, algorithms exploit consumers' decision-making processes through nudges, or behavioral prompts, and dark patterns. Nudges account for psychological, social, cognitive, emotional, and economic factors. In this regard, Thaler and Sunstein (2008) explain that a nudge is an intervention that predictably alters people's behavior without prohibiting options or significantly changing economic consequences.

Dark patterns, in turn, are choice architectures that unethically steer users toward actions that serve suppliers' interests. They rely on false premises, manipulate consent, direct user behavior, and reinforce algorithmic determinism. These tools affect and interfere with consumers' right to choose and, from a collective perspective, may exacerbate disparities. After all, if an algorithm predicts an individual's future in a deterministic manner and treats the person according to that prediction, any departure from the algorithmically prescribed course of action defies the calculated probabilities (Agrassar, 2025). Ultimately, belief in consumers' freedom of decision-making is associated with “a lack of awareness of how this intricate network of influences operates” (Agrassar, 2025, p. 196).

3 Algorithmic determinism and its sociopolitical impact: considerations

Algorithmic determinism refers to the use of algorithms before consumers make decisions for the purpose of identifying patterns and predicting and influencing future decisions. When produced by AI, this determinism affects

human individuality by depriving people of decision-making rationality, autonomy, and the freedom to defy predictions and differ from others (Verbicaro, 2023).

Algorithms seek to create an illusory equality among consumers (Agrassar, 2025). Consequently, consumers' freedom of choice becomes illusory because their identities are categorized into profiles that determine how they are expected to behave on digital platforms (Carvalho; Franco Neto; Verbicaro, 2024). By replicating structures that disregard diversity, this interference with consumer choices may have harmful effects on society (Agrassar, 2025).

From this perspective, a new concept known as "algorithmic colonization" emerges (Agrassar, 2025). It refers to the process of appropriating and exploiting data as a new resource by combining the predatory practices of historical colonialism with the abstract quantification of computational methods (Couldry; Mejias, 2019).

This dynamic extends the global exploitation that began with historical colonialism (Couldry; Mejias, 2019). Determinism and standardization therefore function as an "instrument of algorithmic colonization," which seeks to create an illusory equality among consumers (Agrassar, 2025, p. 196).

The success of digital platforms depends on their ability to predict and influence consumer behavior by determining the choices available to consumers. This process results in voluntary submission to coercive techniques and the erosion of autonomy. In other words, algorithmic colonization seeks to create an illusory equality among consumers, subordinating individual freedom to the logic of markets and surveillance (Verbicaro, 2023, p. 144). Technological surveillance therefore threatens freedom, equality, democracy, and autonomy (Véliz, 2021, p. 25). Algorithmic determinism may consequently compromise diversity by disregarding certain social groups or cultural and local patterns.

In the context of consumption, algorithmic determinism extends beyond the mere optimization of sales. It may become a powerful instrument of social control that reproduces and deepens historical inequalities.

3.1 Algorithmic discrimination

The most harmful manifestation of determinism is algorithmic discrimination. This form of discrimination occurs when algorithms engage in "discriminatory or exclusionary conduct toward human beings" based on gender, race, or geographic origin (Agrassar, 2025, p. 198).

In this regard, the belief that AI is impartial is called into question by the existence of machine bias (Elias, 2017). Discrimination is not inherent in the mathematical structure of an algorithm; rather, it is introduced through biases present in the skewed data used to train the machine (Mendes; Mattiuzzo, 2019). These human biases are "inadvertently" incorporated into machine-learning models, perpetuating "historical discrimination in automated decisions" (Barocas; Selbst, 2016, p. 685). By relying on biased datasets, AI contributes to reinforcing the invisibility of minoritized groups (Agrassar, 2025, p. 198).

Thus, the intersection between discriminatory practices and the predictive capacity of AI gives rise to algorithmic determinism. When applied to consumer relations, suppliers not only predict what consumers want but also determine what they should want, exploiting their vulnerabilities.

Digital platforms therefore induce "micro-behaviors" – small actions suggested and accepted based on browsing histories – to relieve individuals of responsibility for decision-making (Agrassar, 2025, p. 196). If an algorithm classifies a consumer as "vulnerable" or "impulsive," it may target that person with offers of credit carrying excessive interest rates or advertisements for online betting to maximize profitability (Verbicaro; Costa, 2024).

From this perspective, consumers, who are expressly recognized as vulnerable under Article 4, item I, of the CDC (Brazil, 1990), become even more vulnerable in the digital environment, a phenomenon that Marques and Mucelin (2022) describe as "structural digital vulnerability." Consumers thus become "glass consumers": transparent to companies that possess their data but unable to see the mechanisms used to manipulate them (Lace, 2005; Vieira, 2021, p. 10). Furthermore, algorithms render minoritized groups invisible or place them at a disadvantage in the consumer marketplace (Agrassar, 2025).

Algorithmic discrimination is not an abstract concept, as it materializes through restrictions on access to goods and services. For example, the "pink tax" is a phenomenon in which products marketed to women cost more than comparable products marketed to men without any technical justification for the difference (Ricco; Oliveira, 2017, p. 111).

In the digital environment, profiling intensifies this form of gender discrimination. Algorithms identify women as "household managers" or "holistic shoppers" and inundate them with advertisements for cleaning products, beauty products, and household goods, thereby reinforcing sexist stereotypes that portray domestic care as an exclusively

female responsibility (Verbicaro et al., 2020, p. 252). This segmentation not only economically exploits women by charging higher prices for beauty products amid unattainable aesthetic pressures (Wolf, 2018, p. 17), but also restricts their freedom of choice by limiting the content shown to them to a stereotyped niche.

Another form of algorithmic discrimination occurs through geopricing, or location-based pricing. For example, Civil Investigation No. 347, initiated in Rio de Janeiro against the Decolar.com platform, uncovered indications that lodging offers were manipulated based on users' geographic origins (Chagas; Lage, 2020). Upon identifying a consumer's Internet Protocol (IP) address location, the algorithm concealed lower-priced offers or increased prices for certain regions, segregating consumers based on their presumed financial capacity or geographic origin.

Digital discrimination typically arises from the use of biased or incomplete datasets because human biases are inadvertently incorporated into machine-learning models during the selection and labeling of training data. This process consequently perpetuates historical discrimination in automated decisions (Barocas; Selbst, 2016, p. 685).

In summary, the correlation between discriminatory algorithmic biases and algorithmic determinism reveals a mechanism that perpetuates inequality, extends beyond the technical sphere, and directly affects consumer dignity.

This process deprives individuals of the opportunity for self-determination and free choice, confining them to immutable digital profiles that dictate their consumption options and access to services. Consequently, consumer vulnerability is exacerbated and transformed into structural algorithmic vulnerability, primarily compromising two fundamental consumer rights expressly established in the CDC (Brazil, 1990): the rights to choose and to receive information.

3.2 The impact of AI on consumers' right to choose

Capitalism has emerged as a political and financial system that unilaterally claims human experience as free raw material to be converted into behavioral data (Verbicaro, 2023, p. 6). In this context, routine surveillance, which generates profit and power, has become normalized and is intrinsically linked to surveillance capitalism (Sampaio et al., 2021).

In this regard, Zuboff (2020) explains that surveillance capitalism unilaterally transforms human experience into behavioral data. While some of these data are used to improve products, the behavioral surplus feeds "machine intelligence," creating prediction products that anticipate individuals' future actions (Zuboff, 2020, p. 18). The current landscape is defined by the digital economy, which is characterized by dynamic competition, continuous cycles of innovation and disruption, and reliance on data-driven innovation (Bagnoli, 2022, p. 505-506).

Human behavior – specifically consumer behavior for the purposes of this study – thus becomes a commodity (Carvalho; Franco Neto; Verbicaro, 2024, p. 154); that is, Big Tech companies predict and influence users' every action (Verbicaro, 2023, p. 7). In this context, scholars have recognized the existence of algorithmic consumer vulnerability (Verbicaro, 2023; Carvalho; Franco Neto; Verbicaro, 2024; Chaves, 2025).

Algorithmic vulnerability arises from consumers' susceptibility within the virtual environment (Verbicaro; Costa, 2024). It refers to the possibility that suppliers may use their informational power to exploit personal data and erode individual choice (Verbicaro; Costa, 2024) since data processing – including collection, analysis, and handling – occurs without consumers' necessary consent or knowledge. Suppliers' processing of data therefore ultimately manipulates user choices.

This situation creates a technical and informational imbalance. Because consumers generally lack knowledge of programming languages (Martins; Longhi; Faleiro Junior, 2022), they can be identified and tracked as they navigate digital networks, becoming "glass consumers."

Algorithmic consumer profiling involves appropriating consumers' habits through the collection of their data, thereby creating a "fatalistic and illegitimate social profile" that may result in discriminatory conduct (Agrassar, 2025) against certain consumer groups. In other words, profiling predicts an individual's future and causes that person to be treated according to the prediction. Ultimately, AI prevents individuals from acting freely and defying calculated probabilities (Verbicaro, 2023).

Conversely, personal data have come to be recognized as a fundamental right. Protecting users' fundamental rights to privacy and personal data protection has therefore assumed an essential role. Constitutional Amendment No. 115 (Brasil, 2022), which added item LXXIX to Article 5 of Brazil's Federal Constitution, elevated personal data protection to the status of a fundamental right. This provision reinforces the government's duty to protect individuals from arbitrary digital interference and guarantee the free formation of their will.

Moreover, personal data protection is connected to the free development of personality (Pasquale, 2015). This right is reflected in the principle of informational self-determination established in Article 1, item II, of the LGPD (Brasil, 2018) and in the principle of human dignity, a cornerstone of the Brazilian Federal Constitution under Article 1, item III (Brasil, 1988), because each human being possesses inherent value and must not be treated merely as an object of statistical predictions.

Article 6, item II, of the CDC (Brasil, 1990) recognizes the fundamental right to “freedom of choice and equality in contractual relationships.” This provision ensures that consumers must actively direct their own decisions rather than passively receive technological inducements. When consumers cannot exercise this freedom, their vulnerability is exacerbated.

To mitigate this situation, Article 20 of LGPD (Brasil, 2018) provides a mechanism of resistance by guaranteeing data subjects the right to request a review of decisions made exclusively through the automated processing of personal data that affect their interests, including decisions intended to define their personal or consumer profiles. The so-called right to an explanation seeks to restore consumers’ basic understanding of how their choices are being constrained.

Indeed, combating submission to the logic of markets and surveillance – which transforms individuals into “livestock, into animals of consumption and data” (Han, 2022, p. 7) – requires restoring individual freedom as a political value (Verbicaro, 2023, p. 144). This freedom is inseparable from algorithmic transparency, a duty analogous to the right to clear and adequate information about products and services under Article 6, item III, of CDC (Brasil, 1990). Without information explaining why a particular product is offered and why others are excluded, the right to choose becomes a legal fiction.

Furthermore, the intersection of algorithmic determinism and human rights reveals a new dimension of consumer vulnerability: the threat to psychological integrity. The CDC was designed primarily to protect consumers’ health and physical safety under Article 6, item I (Brasil, 1990). However, interactions with cyberspace require a broader interpretation that encompasses mental health as a legally protected interest safeguarded against abusive and manipulative commercial practices.

3.3 Two fundamental consumer rights at risk: the right to information and the right to protection against advertising strategies (Article 6, items III and IV, of CDC)

Digital advertising strategies designed to capture consumer intent have become increasingly intensive. According to data from the Brazilian Advertising Standards Forum (CENP), 40.2% of companies’ total advertising investment – covering approximately 327 advertising agencies – is allocated to online digital media (Pezzotti, 2025). These practices reflect an effort to personalize advertising through the increased use of technologies supported by algorithms. Various consumer goods and services are therefore associated with consumers’ desires and intentions in a targeted and personalized manner based on their data and profiles, even to the point of attempting to induce them to change their consumption experiences.

From this perspective, access to personal data compromises consumer protection. Sousa and Vieira (2021) argue that consumer autonomy is connected to the ability to choose; however, “algorithms are designed to influence user behavior and reflect only the interests of third parties rather than those of the data subjects, replacing users’ preferences with what the algorithm has inferred” (Sousa; Vieira, 2021).

An important dilemma must be acknowledged. On the one hand, consumers are concerned about their personal data and privacy; on the other, algorithms may help prevent them from receiving unwanted advertising messages. Which outcome do consumers prefer? While this question remains unresolved, the strategies through which these practices operate can be objectively examined. Suppliers’ conduct demonstrates a failure to respect consumers’ fundamental right to protection under Article 6, item II, of CDC (Brasil, 1990).

Likewise, as the capture and collection of information left behind by consumers increase, consumers remain unaware of and uninformed about suppliers’ activities. It should be noted that the consumer right to information is established in several provisions of the CDC (Brasil, 1990) and applies at multiple stages of the contractual relationship. According to Bessa (2022), these provisions first encompass product-related information under Articles 8, 10, and 12 and problems arising from inadequate product information under Articles 18 and 20. They also include information associated with offers under Articles 30, 31, and 35, as well as information required at subsequent stages of the contractual relationship under Articles 39, 42, 46, 48, and 51, item IV.

The right to information is therefore an essential fundamental right in consumer relations, and its importance increases as consumption becomes more sophisticated through disruptive technologies. Safeguarding this right is indispensable, particularly in the context of advertising, which uses AI-based technologies and algorithms to expand markets – a practice that undoubtedly affects the fundamental right to information.

4 Explainability and transparency for consumer protection

The preceding sections established that algorithmic determinism and algorithmic colonization thrive in an environment of informational opacity, where manipulation and discrimination proliferate without detection (Agrassar, 2025).

Reversing the erosion of consumer autonomy therefore requires legal mechanisms that ensure system transparency and accountability. The focus must consequently shift from mere technological effectiveness to ethics and human dignity (Verbicaro, 2023; Zuboff, 2020).

The primary obstacle to the oversight of AI systems and the attribution of responsibility for their outcomes is the so-called black-box problem (Santos, 2025). Automated decisions made by these systems frequently provide no clear and comprehensible explanation of how a particular outcome was reached (Santos, 2025).

Algorithmic opacity has three dimensions: i) epistemic opacity, which arises from the complexity of AI and its capacity to identify patterns across an unimaginable number of variables, making the system's logic extremely difficult or impossible for the human mind to understand (Nogarolli; Faleiros Júnior, 2021); ii) nondisclosure opacity, which results from corporate or government secrecy, whereby the sharing of specific code or datasets is prohibited to protect trade or industrial secrets (Nogarolli; Faleiros Júnior, 2021, p. 174); and iii) explanatory opacity, which concerns the difficulty of translating the logic underlying a technology's operation into language that can be understood by ordinary users without technical programming knowledge (Nogarolli; Faleiros Júnior, 2021; Abrusio, 2022).

The information crisis created by this opacity allows biases and discrimination to proliferate without detection (Agrassar, 2025). Transparency is therefore regarded as a fundamental condition for ensuring accountability in public discourse on governance (Santaella, 2021). According to the European Parliament (2017), transparency is intended to ensure that users understand when they are interacting with AI systems and should encompass the logic underlying the system's operation, the categories of people affected, and the risks involved.

In this context, the right to an explanation emerges as a legal mechanism for overseeing automated decisions based on profiles and predictions, requiring systems to be transparent. However, Franzolin, Monteiro, and Laurentis (2025) argue that the effective implementation of this right may encounter difficulties⁴.

Brazilian law, through the LGPD (Brasil, 2018), guarantees data subjects the right to request a review of decisions made exclusively through the automated processing of personal data that affect their interests, particularly decisions intended to define their personal, professional, or consumer profiles (Brasil, 2018, Article 20).

LGPD therefore requires data controllers to provide clear, adequate information regarding the criteria and procedures used in automated decision-making (Brasil, 2018, Article 20). This right serves as a "link between distinct regulatory modalities" (Frazão; Goettenauer, 2020, p. 59), translating elements of the mathematical infrastructure into natural language (Frazão; Goettenauer, 2020, p. 59). This concept is complemented by the duty-based principles of accountability and answerability established in Article 6, item X, of the LGPD (Rosenvald; Faleiros Júnior, 2021, p. 777).

Accountability entails adopting effective measures capable of demonstrating compliance with data-protection standards (Facchini Neto; Soares, 2021) and requires human monitoring of algorithms based on ethical and legal considerations (Agrassar, 2025). Explainable AI (XAI), in turn, refers to a technical approach intended to make the decisions of AI models interpretable and comprehensible to users, regardless of their programming knowledge (Abrusio, 2022). An XAI model helps users understand "why this output was produced for this input" (Russell; Norvig, 2022, p. 644).

⁴ Vale ressaltar que o direito à explicação pode também se apresentar como óbice para se concretizar. Nesse sentido, vale destacar que a "A falta de *explicabilidade* nos sistemas de IA levanta sérias questões sociais e éticas, principalmente em relação à transparência e à responsabilidade. Quando não é possível a compreensão dos processos de tomada de decisão, torna-se difícil para os desenvolvedores e reguladores identificarem e corrigir os possíveis vieses e equívocos que podem resultar em decisões discriminatórias que favorecem certos grupos em detrimento de outros como retro exemplificado. De igual forma, uma vez que indivíduos podem ser impactados por decisões automatizadas sem saber como ou por que elas foram tomadas, o exercício de direitos fundamentais, como o direito à informação e ao contraditório, podem, por vezes, serem prejudicados. Nesta perspectiva, acrescenta-se que, decisões automatizadas também podem trazer implicações sociais e éticas; mas o foco deste trabalho é contribuir para a discussão sobre a viabilidade do direito à explicação acerca das decisões tomadas por sistemas de IA" (Franzolin; Monteiro; Laurentis, 2025).

For meaningful explanations to be possible, market participants must establish a preventive governance framework. Such measures are known as *ex ante* regulation because they seek to prevent risks and harm before violations occur (Agrassar, 2025; Santos, 2025). Risk regulation must be the central element of this framework, connecting the collection of information and identification of risks to the development of preventive mechanisms (Cantarini, 2021).

AI governance and digital compliance also play important roles in mitigating risk (Santos, 2025, p. 81), as they require organizations to establish mechanisms for compliance with ethical and legal standards (Verbicaro, 2023, p. 144).

The principal instrument for documenting and demonstrating compliance is algorithmic impact assessment (AIA), which is crucial for high-risk systems (Vainzof; Sefarino; Steinwascher, 2022, p. 256). AIA maps the risks, benefits, reliability, and transparency of AI systems and is essential for monitoring and accountability purposes (Vainzof; Sefarino; Steinwascher, 2022). Bill No. 2,338 (Brazil, 2023), which addresses the regulation of AI in Brazil, establishes AIA as a requirement for high-risk systems.

In complex systems, human-in-the-loop intervention is a necessary component of decision review (Kleinberg et al., 2018). The value of human oversight lies in the ability to identify exceptional contexts and consider factors that automated systems cannot adequately process (Kleinberg et al., 2018, p. 240).

The Brazilian National Data Protection Authority (ANPD) serves as the key authority on AI and data protection and promotes responsible innovation (ANPD, 2023). Its activities should pursue responsive regulation that incorporates dialogue among government authorities, civil society, and the business sector (Verbicaro; Agrassar, 2024). By strengthening the ANPD's authority and imposing transparency and accountability obligations on the use of AI, the legal system can build a more ethical, equitable, and dignified digital future for consumers (Agrassar, 2025).

Although there are legal instruments to mitigate consumer vulnerability in the digital environment (Klausner, 2015, p. 67), the outlook has not been so optimistic since big techs still concentrate intense economic power, with revenues exceeding the gross domestic product (GDP) of some countries.

Moreover, an aggravated informational asymmetry is observed in the virtual environment. This asymmetry is justified by the fact that consumers' personal data become suppliers' "raw material," whose access is continuously expanded and instrumentalized through algorithms.

Certainly, the implementation of AI in the design of public policies can bring direct benefits to consumers by promoting more conscious choices. An example highlighted by the Organisation for Economic Co-operation and Development (OECD, 2019) concerns the use of smart meters in the electric power sector. Studies have shown that the instantaneous availability of data on consumption and rates allowed consumers to make more informed decisions, reducing energy use during peak hours and lowering costs, which constitutes an efficient public policy based on behavioral insights.

As stated by Domingues (2021, p. 14), Brazil's consumer protection public policy has operated through the National Consumer Secretariat (SENACON). This agency has used Technical Notes to curb AI-based and data-collection abuses, filling legislative gaps. Notable is the conviction of a large retail chain (pharmacy/fashion) for using facial recognition cameras to capture consumers' reactions to advertisements without consent (Brasil, 2019). On that occasion, Article 39 of CDC (Brasil, 1990) was cited, which prohibits suppliers of products or services from "IV – taking advantage of the consumer's weakness or ignorance, considering their age, health, knowledge, or social condition, to impose their products or services on them." SENACON found that the practice violated the duty of information and objective good faith, characterizing the processing of biometric data without transparency as an abuse of rights.

Therefore, effective public policy cannot be merely reactive (*ex post*). It is imperative to adopt *ex ante* (preventive) regulation, based on AIA and compliance reports. Such instruments, inspired by standards of the OECD and the National Institute of Standards and Technology (NIST), make it possible to map risks and biases before the product reaches the market, shifting the focus from mere technological efficiency to ethics and human dignity.

In light of this, for the national consumer relations policy to be effective in the virtual environment, the State must strengthen platform oversight mechanisms, promote consumer digital education, and update normative interpretation to curb algorithmic harassment and manipulation.

5 Conclusions

This study demonstrated that the rise of AI and the consolidation of platform capitalism have transmuted traditional consumer vulnerability into a structural digital vulnerability. The central research problem revealed that algorithmic determinism acts as a vector of technical control that, by processing past data to anticipate future behaviors, severely restricts individuals' decision-making freedom. The fundamental right to choose, established by CDC (Brasil, 1990), is reduced to an illusory freedom in which the consumer is "chosen" through micro-behaviors captured and induced by opaque choice architectures.

As extensively demonstrated by the literature review addressed in this work, the architecture of the contemporary digital market has converted the consumer into a mere datafied asset, significantly compromising their right to information. This reality shows how the principle of vulnerability, as part of the National Consumer Relations Policy (Brasil, 1990, art. 4), becomes more ostensive in a digital environment invaded by disruptive digital tools, such as AI, used to better track consumer choices. The consumer does not exercise the right to choose; in fact, they become induced, chosen, and conditioned toward this or that advertising message or product.

In sum, research highlighted that the 21st century is transforming private and consumer relations, now structured within a digital environment of increasing capture of information and processing of personal data collected from consumers, which occurs through the tool of AI. In this scenario, this study sheds light on relevant issues of privacy and personal data protection, revealing the complexity that permeates this data collection and the use of digital means.

Beyond mere collection, the profiling of personal data presents growing surveillance and computational analysis of consumer data, made available to the market by suppliers. In this sense, there is a worsening of consumer vulnerability.

Therefore, emphasis was placed on the dogmatics of algorithmic determinism and the pursuit of consumer protection through the right to explainability. However, in line with prior research, that this institute is still insufficient to curb the commodification of human behavior based on collected personal data.

Thus, the central contribution of this study lies in the premise that the current reactive structure of the Brazilian legal system is ineffective in protecting digital dignity. An unavoidable transition to ex ante governance model is required, valuing reports and effective, transparent access to data that suppliers collect from consumers.

In summary, there is no neutrality but rather a growing algorithmic colonization. By using biased databases, algorithms replicate and automate historical inequalities of race, gender, and class. Hence the emphasis on discriminatory practices known as "pink tax," "geopricing," and the exploitation of profiles considered vulnerable or impulsive through dark patterns, transforming the promise of personalization into a tool of segregation and social control.

It is critically observed that the Judiciary itself, at times, acts as a legitimizer of algorithmic opacity. A clear example of this failure is the enactment of Precedent 550 of the Superior Court of Justice (STJ), which authorizes financial institutions to use credit scoring systems, dispensing with prior consumer consent (Brasil, 2014). By validating this practice under the justification that it is a "mere statistical calculation," the court ignores the harmful consequences of algorithmic discrimination, sanctioning a system that marginalizes and excludes low-income consumers from access to credit. Moreover, this system perpetuates the cycle of commodification of personal data – in the case of this study, consumers' data – and intensifies social inequalities, aggravating the lack of transparency in suppliers' strategies for collecting personal data to expand their markets.

Given this protective gap, this article argues that overcoming "illusory freedom" will not occur solely through the isolated application of CDC (Brasil, 1990). It proposes the application of a systematic and coordinated interpretation, along with greater effectiveness of the right to an explanation of automated decisions (Brasil, 2018).

As a means of mitigating the state of algorithmic harm, the research points to the need for ex ante governance that shifts the focus from mere market efficiency toward the protection of human dignity. Explainability and transparency emerge as tools to overcome the "black-box problem," ensuring that automated decisions are interpretable and subject to human review. However, it should be noted that this explainability faces limits in human capacity, which is often unable to clarify how the decision was reached by the AI. Digital compliance structures, such as the AIA, and the strengthening of the duty of accountability are essential to ensure that technological development respects fundamental rights and informational self-determination.

Thus, resistance to the standardization imposed by technological surveillance requires that freedom be reaffirmed as a political value against the extractivist logic of capital. Only through a regulatory model that prioritizes

transparency and ethics will it be possible to guarantee an equitable digital future, preserving individuality and the free development of human personality in the face of the arbitrariness of the algorithmic era.

The absence of transparency and explainability in AI systems should establish an absolute presumption of abusive practice and defect in service provision (Brasil, 1990), reversing the burden of proof. It is not up to the consumer to decipher the “black box” to prove that they were manipulated or discriminated against; on the contrary, it is the supplier’s obligation to present prior algorithmic impact reports and demonstrate the adoption of digital compliance and ethical audit measures (e.g., human-in-the-loop), under penalty of civil and administrative liability.

Therefore, AI regulation in Brazil cannot be limited to voluntary ethical guidelines (soft law). In this sense, this research shows that the Law contributes to imposing strict limits on “surveillance capitalism.” Furthermore, algorithmic transparency must be guaranteed, and explanations in natural language must be made mandatory, translating the mathematical infrastructure of the codes – which is not an obstacle to technological innovation, but rather the only way to reestablish instrumental citizenship and rescue human beings from their condition as hostages to the profit-driven machinery of major platforms.

References

- ABRUSIO, Juliana. O princípio da Inteligência Artificial Explicável e a Proteção de Dados. In: RAIS, Diogo; ABRUSIO, Juliana (org.). **Privacidade, mercado e cidadania: uma conexão a partir da IA**. São Paulo: Revista dos Tribunais, 2022.
- ABRUSIO, Juliana. **Proteção de Dados na Cultura do Algoritmo**. 1. ed. São Paulo: D’Plácido, 2020.
- AGRASSAR, Hugo José de Oliveira. Resenha do livro “Algoritmos de consumo: discriminação, determinismo e solução online de conflitos na era da inteligência artificial”, de Dennis Verbicaro. **Revista IBERC**, Belo Horizonte, v. 8, n. 2, p. 195-200, 2025.
- BAGNOLI, Vicente. **Direito econômico e concorrencial: o poder econômico e seus limites jurídicos**. 9. ed. São Paulo: Thomson Reuters Brasil, 2022.
- BAROCAS, Solon; SELBST, Andrew. Big Data’s Disparate Impact. **California Law Review**, [S. l.], v. 104, p. 671-732, 2016. DOI: <https://doi.org/10.2139/ssrn.2477899>. Disponível em: <https://ssrn.com/abstract=2477899>. Acesso em: 14 mai. 2026.
- BESSA, Leonardo Roscoe. **Código de defesa do consumidor comentado**. 2. ed. São Paulo: Revista do Tribunais, 2022.
- BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 jul. 2026.
- BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 14 mai. 2026.
- BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 14 mai. 2026.
- BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 mai. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional do Consumidor. Departamento de Proteção e Defesa do Consumidor. **Nota Técnica n.º 101/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ**. Processo nº 08012.005555/2015-13. Brasília, DF: Ministério da Justiça e Segurança Pública, 2019. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/notas-tecnicas/anexos/nota-tecnica-101.pdf>. Acesso em: 14 mai. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional do Consumidor. Departamento de Proteção e Defesa do Consumidor. **Nota Técnica n.º 32/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ**. Processo nº 08012.000723/2018-19. Brasília, DF: Ministério da Justiça e Segurança Pública, 2019. Disponível em: https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/defesadoconsumidor/Biblioteca/notas-juridicas-upload/13-13810396_nota_tecnica_32_2019_cgctsa_dpdc_senacon_mj.pdf. Acesso em: 30 mai. 2026.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Autoria: Senador Rodrigo Pacheco. Brasília, DF: Senado Federal, 2023. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1742240889313&disposition=inline>. Acesso em: 27 nov. 2023.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.419.697 - RS (2013/0386285-0)**. Relator: Ministro Paulo de Tarso Sanseverino. Julgado em: 28 out. 2014. Publicado em: 17 nov. 2014. Disponível em: <https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?O=JT&b=ACOR&livre=201303862850>. Acesso em: 30 mai. 2026.

CANTARINI, Paola. Inteligência artificial: desafios regulatórios e risquificação. In: PINHO, Anna Carolina *et al.* (org.). **Discussões sobre Direito na Era Digital**. 1. ed. Rio de Janeiro: GZ, 2021. p. 547-556.

CAPGEMINI RESEARCH INSTITUTE. **From hype to habit: How consumers are embracing AI**. [S. l.]: Capgemini, 2025. Disponível em: <https://www.capgemini.com/br-pt/insights/biblioteca-de-pesquisas/ia-e-consumidores-2025/>. Acesso em: 30 mai. 2026.

CARVALHO, Anna Costa; FRANCO NETO, Édson Raymundo Pinheiro de Souza; VERBICARO SOARES, Dennis. Perfilização e Determinismo Algorítmico: impactos na autonomia e liberdade do consumidor digital. **Revista Jurídica do Cesupa**, [S. l.], v. 5, n. 2, p. 147–169, 2024.

CHAGAS, Ciro Costa; LAGE, Lorena Muniz. A opacidade gerada pelos algoritmos e inteligência artificial e a consequente necessidade de regulamentações. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (org.). **O Direito Civil na era da inteligência artificial**. São Paulo: Revista dos Tribunais, 2020.

CHAVES, Fernanda Silveira. A hipervulnerabilidade do consumidor diante da inteligência artificial no contexto da modernidade líquida. Goiânia: **Revista Aracê**, [S. l.], v. 7, n. 4, p. 17836, 2025. DOI: <https://doi.org/10.56238/arev7n4-128>. Disponível em: <https://periodicos.newsciencepubl.com/arace/article/view/4397>. Acesso em: 30 maio 2026.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros**: TIC Domicílios 2024. São Paulo: Cetic.br; NIC.br, 2025. Disponível em: https://cetic.br/media/docs/publicacoes/2/pt-br/20251027170648/tic_domicilios_2024_livro_eletronico.pdf. Acesso em: 30 mai. 2026.

COULDRY, Nick; MEJIAS, Ulises. **The costs of connection**: how data is colonizing human life and appropriating it for capitalism. Stanford: Stanford University Press, 2019.

DOMINGUES, Juliana Oliveira; SILVA, Alais Aparecida Bonelli da; SOUZA, Henrique Monteiro Araujo de. Inteligência artificial nas relações de consumo: reflexões à luz do histórico recente. In: VAINZOF, Rony (org.). **Inteligência artificial**: sociedade, economia e Estado. São Paulo: Thomson Reuters Brasil, 2021.

ELIAS, Paulo Sá. **Algoritmos, Inteligência Artificial e o Direito**. [S. l.]: Consultor Jurídico, 2017. Disponível em: <https://www.conjur.com.br/wp-content/uploads/2023/09/algoritmos-inteligencia-artificial.pdf>. Acesso em: 14 mai. 2026.

FACCHINI NETO, Eugênio; SOARES, Flaviana Rampazzo. Responsabilidade Civil pela Violação ao Dever de Proteção de Dados na LGPD. In: PINHO, Anna Carolina *et al.* (org.). **Discussões sobre direito na era digital**. 1. ed. Rio de Janeiro: GZ, 2021.

FRANZOLIN, Cláudio José; MONTEIRO, Giovanna Voorn; LAURENTIS, Lucas Catib de. A (in)existência de um direito à explicação de decisões automatizadas. **THEMIS: Revista da Esmec**, [S. l.], v. 23, n. 1, p. 65–91, 2025. DOI: <https://doi.org/10.56256/themis.v23i1.1103>. Disponível em: <https://revistathemis.tjce.jus.br/index.php/THEMIS/article/view/1103>. Acesso em: 7 mar. 2026.

FRAZÃO, Ana; GOETTENAUER, Carlos. O jogo da imitação jurídica: o direito à revisão de decisões algorítmicas como um mecanismo para a necessária conciliação entre linguagem natural e infraestrutura matemática. In: SILVA, Rodrigo da Guia; TEPEDINO, Gustavo. (org.). **O Direito Civil na Era da Inteligência Artificial**. 1. ed. São Paulo: Thomson Reuters, 2020.

GOLDENBERG, Mirian. O corpo como capital: para compreender a cultura brasileira. **Arquivos em Movimento**, Rio de Janeiro, v. 2, n. 2, 2006.

HAN, Byung-Chul. **Psicopolítica**: neoliberalismo e novas técnicas de poder. Lisboa: Relógio D'água, 2015.

HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Petrópolis: Vozes, 2022.

KAHNEMAN, Daniel; SIBONY, Olivier; SUNSTEIN, Cass R. **Ruído**. Tradução: Cássio de Arantes Leite. 1. ed. Rio de Janeiro: Objetiva, 2021.

KLAUSNER, Eduardo Antônio. A globalização e a proteção do consumidor brasileiro. **Revista dos Tribunais**, [S. l.], v. 97, 2015.

KLEINBERG, Jon *et al.* Human decisions and machine predictions. **The Quarterly Journal of Economics**, [S. l.], v. 133, n. 1, p. 237-293, 2018.

LACE, Susanne. **The glass consumer**: life in a surveillance society. Bristol: Policy Press, 2005.

LEWIS, Paul; HILDER, Paul. Leaked: Cambridge Analytica's blueprint for Trump victory. **The Guardian**, [S. l.], 23 mar. 2018. Disponível em: <https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory>. Acesso em: 7 mar. 2026.

MARQUES, Claudia Lima; MUCELIN, Guilherme. Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor. **Civilistica.com: Revista Eletrônica de Direito Civil**, [S. l.], v. 11, n. 3, p. 1-30, 2022. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/872>. Acesso em: 7 mar. 2026.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados Pessoais**: Lei 13.709/2018. 1. ed. São Paulo: Foco, 2022.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação algorítmica: conceito, fundamento legal e tipologia. **Revista de Direito Público**, [S. l.], v. 16, n. 90, p. 1-26, 2019. Disponível em: www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766. Acesso em: 15 fev. 2026.

NOGAROLLI, Rafaella; FALEIROS JÚNIOR, José Luiz de Moura. Tripla dimensão semântica da opacidade algorítmica e seus reflexos na responsabilidade civil médica. In: CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL, 2., 2021, Belo Horizonte. **Anais [...]**. Belo Horizonte: Skema Business School, 2021.

NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição da função decisória às máquinas. **Revista de Processo**, [S. l.], v. 43, n. 285, p. 421-447, nov. 2018.

OLIVA, Afonso Carvalho de; PESSOA, Flávia Moreira Guimarães. Bancos de Dados e a Proteção do Consumidor Brasileiro: o Panóptico Pós-Moderno. **Prima Facie**, [S. l.], v. 15, n. 28, p. 01–43, 2016.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Delivering better policies through behavioural insights**. Paris: OECD Publishing, 10 abr. 2019. Disponível em: https://www.oecd-ilibrary.org/governance/delivering-better-policies-through-behavioural-insights_6c9291e2-en. Acesso em: 30 dez. 2023.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Framework for the Classification of AI Systems**. Paris: OECD Publishing, 22 fev. 2022. (OECD Digital Economy Papers). Disponível em: https://www.oecd.org/en/publications/oecd-framework-for-the-classification-of-ai-systems_cb6d9eca-en.html. Acesso em: 30 dez. 2023.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Governing with Artificial Intelligence**. Paris: OECD Publishing, 13 jun. 2024. (OECD Artificial Intelligence Papers). Disponível em: https://www.oecd.org/en/publications/governing-with-artificial-intelligence_26324bc2-en.html. Acesso em: 30 dez. 2023.

PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém **recomendações à Comissão sobre disposições de Direito Civil sobre Robótica (2015/2103(INL))**. Estrasburgo, 16 fev. 2017. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52017IP0051>. Acesso em: 30 dez. 2023.

PASQUALE, Frank. **The Black Box Society: The Secret Algorithms That Control Money and Information**. Cambridge, MA: Harvard University Press, 2015.

PEREIRA, Laudelina Leonardo. Score de crédito: relações entre as inferências no mercado de dados pessoais e a desigualdade na sociedade. In: ENCONTRO ANUAL DA ANPOCS, 44., 2020, São Paulo. **Anais eletrônicos [...]**: GT04 - Capitalismo, reconhecimento e desigualdade. São Paulo: ANPOCS, 2020. Disponível em: <https://anpocs.org.br/2020/12/01/44o-encontro-anual-da-anpocs/>. Acesso em: 7 mar. 2026.

PEREIRA, Thales Alessandro Dias. Transparência de algoritmos e decisões automatizadas: compreendendo o art. 20 da LGPD. In: PEIXOTO, Fabiano Hartmann (org.). **Inteligência artificial: estudos de inteligência artificial**. Curitiba: Alteridade, 2020.

PEREIRA, Uiara Vendrame; TEIXEIRA, Tarcísio. Inteligência artificial: a quem atribuir responsabilidade?. **Revista de Direitos e Garantias Fundamentais**, [S. l.], v. 20, n. 2, p. 119–142, 2019. DOI: <https://doi.org/10.18759/rdgf.v20i2.1523>. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1523>. Acesso em: 11 jun. 2026.

PEZZOTTI, Renato. Investimento em mídia no Brasil alcançam R\$ 11,9 bi no 1º semestre de 2025. **UOL**, São Paulo, 12 set. 2025. Disponível em: <https://economia.uol.com.br/noticias/redacao/2025/09/12/cenp-meios-investimentos-em-midia-alcancam-r-1193-bi-no-1-semester-de-2025.amp.htm>. Acesso em: 14 mai. 2026.

QUIJANO, Aníbal. Colonialidade do poder e classificação social. In: SANTOS, Boaventura de Sousa; MENESES, Maria Paula (org.). **Epistemologias do Sul**. Coimbra: Edições Almedina, 2009.

RICCO, Adriana S.; OLIVEIRA, Débora B. A influência do marketing e o comportamento da consumidora no processo de compra de produtos com taxa rosa. **Espaço e Tempo Midiáticos: Revista do Grupo de Pesquisa Mídias e Territorialidades Ameaçadas**, [S. l.], v. 2, n. 1, p. 111-126, 2017.

ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. Accountability e a mitigação da responsabilidade civil na Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e políticas de proteção de dados**. São Paulo: Ed. RT, 2021.

RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência Artificial: uma abordagem moderna**. Tradução: Daniel Vieira; Flávio Soares Corrêa da Silva. 4. ed. Rio de Janeiro: LTC, 2022.

SAMPAIO, José Adércio Leite *et al.* Capitalismo de Vigilância e a ameaça aos direitos fundamentais da privacidade e da liberdade de expressão. **Revista Unicuritiba**, Curitiba, v. 1, n. 63, p. 89-113, 2021.

SANTAELLA, Lúcia. Desafios e dilemas da ética na inteligência artificial. In: GUERRA FILHO, Willis Santiago; SANTAELLA, Lúcia; KAUFMAN, Dora; CANTARINI, Paola (org.). **Direito e inteligência artificial**: fundamentos. Rio de Janeiro: Lumen Juris, 2021. v. 1, p. 109-136.

SANTOS, Boaventura de Sousa. Boaventura de Sousa Santos: o Colonialismo e o século XXI. **Centro de Estudos Estratégicos da Fiocruz**, [S. l.], 6 abr. 2018. Disponível em: <https://cee.fiocruz.br/boaventura-o-colonialismo-e-o-seculo-xxi/>. Acesso em: 15 fev. 2026.

SANTOS, Marcelo Fonseca. **Direito de explicação em inteligência artificial**. 2025. Dissertação (Mestrado em Direito Político e Econômico) – Faculdade de Direito, Universidade Presbiteriana Mackenzie, São Paulo, 2025.

SCHIAVI, Iara. As tendências neoliberais e dataficadas da incorporação tecnológica nas cidades. In: SILVEIRA, Sérgio Amadeu da; SOUZA, Joyce; CASSINO, João Francisco (org.). **Colonialismo de dados e modulação algorítmica**. São Paulo: Autonomia Literária, 2021.

SOUZA, Thatianne Silva; VIEIRA, Manuela Corral. Reflexões sobre a publicidade digital algorítmica e programática e os desafios entre relevância e controle. In: COMUNICON, 2021, São Paulo. **Anais [...]**. São Paulo: ESPM, 2021. Disponível em: https://comunicon.espm.edu.br/wp-content/uploads/2021/11/SOUSA_CORRAL.pdf. Acesso em: 15 fev. 2026.

SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da; AVELINO, Rodolfo (org.). **A sociedade do controle**: manipulação e modulação nas redes sociais. São Paulo: Hedra, 2018.

SPAGNOLLO, Leticia; TONIAL, Nadya Regina Gusella. O papel do algoritmo como influenciador na sociedade de consumo e a (hiper)vulnerabilidade do consumidor. **Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo**, [S. l.], v. 9, n. 1, p. 76–95, 2023. DOI: <http://dx.doi.org/10.26668/indexlawjournals/2526-0030/2023.v9i1.9708>. Disponível em: <https://indexlaw.org/index.php/revistadgrc/article/view/9708>. Acesso em: 15 fev. 2026.

THALER, Richard; SUNSTEIN, Cass. **Nudge**: improving decisions about health, wealth, and happiness. New Haven: Yale University Press, 2008.

UNITED STATES. Department of Commerce. **AI Risk Management Framework**. Gaithersburg, MD: National Institute of Standards and Technology, 26 jul. 2024. Disponível em: <https://www.nist.gov/itl/ai-risk-management-framework>. Acesso em: 15 fev. 2026.

UNITED STATES. National Institute of Standards and Technology. **Artificial Intelligence Risk Management Framework**: Generative Artificial Intelligence Profile (NIST AI 600-1). Gaithersburg, MD: NIST, 2024. Disponível em: <https://doi.org/10.6028/NIST.AI.600-1>. Acesso em: 15 fev. 2026.

VAINZOF, Rony; SERAFINO, Danielle; STEINWASCHER, Aline. Aplicações e regulação da inteligência artificial. In: VAINZOF, Rony *et al.* (org.). **Legal Innovation**: o futuro do direito e o direito do futuro. São Paulo: Thomson Reuters, 2022.

VÉLIZ, Carissa. **Privacidade é poder**: porque e como você deveria retomar o controle de seus dados. São Paulo: Editora Contracorrente, 2021.

VERBICARO, Dennis. **Algoritmos de consumo**: discriminação, determinismo e solução online de conflitos na era da inteligência artificial. São Paulo: Ed. RT, 2023.

VERBICARO, Dennis; AGRASSAR, Hugo José de Oliveira. Desafios na regulamentação de algoritmos sob o Marco Civil da Internet. **Revista de Direito do Consumidor**, [S. l.], v. 154, p. 109-131, 2024.

VERBICARO, Dennis; ALCANTARA, Ana Beatriz Quintas Santiago de. A percepção do sexismo face à cultura do consumo e a hipervulnerabilidade da mulher no âmbito do assédio discriminatório de gênero. **Revista Pensamento Jurídico**, São Paulo, v. 11, n. 1, p. 172-192, 2017.

VERBICARO, Dennis; COSTA, Ana Izabelle de Oliveira. O uso do sistema scoring nos serviços bancários: uma análise sobre a (i)licitude da discriminação algorítmica dos consumidores de baixa renda. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, n. 54, p. 137-162, 2024.

VERBICARO, Dennis; LEAL, Pastora Teixeira; ESTEVES, Lorena Meirelles. O mito da beleza e a vulnerabilidade agravada da mulher na sociedade de consumo. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 19, e64495, p. 1-28, 2024.

VERBICARO, Dennis; MARANHÃO, Ney. **Direitos da vulnerabilidade na era do capitalismo de plataforma**. São Paulo: Venturoli, 2022.

VERBICARO, Dennis; MOURA, João Vitor Mendonça de; COSTA, Rosalina Moitta Pinto da. Master of Puppets o determinismo algorítmico, os dark patterns e a urgência no controle das casas de aposta on-line. **Revista de Direito do Consumidor**, [S. l.], v. 157, p. 1-21 2025.

VERBICARO, Dennis; VIEIRA, Janaina do Nascimento. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. **Revista de Direito do Consumidor**, [S. l.], v. 30, n. 134, p. 195-226, 2021.

WOLF, Naomi. **O mito da beleza**: como as imagens de beleza são usadas contra as mulheres. Tradução: Waldéa Barcellos. Rio de Janeiro: Rocco, 2018.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

ZUBOFF, Shoshana. It's not that we've failed to rein in Facebook and Google. We've not even tried. **The Guardian**, [S. l.], 2 jul. 2019. Disponível em: <https://www.theguardian.com/commentisfree/2019/jul/02/facebook-google-data-change-our-behaviour-democracy>. Acesso em: 15 fev. 2026.