Global Network
on Electoral Justice

Regulatory and Judicial Overview of the use of Artificial Intelligence in Electoral Processes

Version: October 2024

General Coordination: Board of the Observatory on Social Media

Editorial Committee: Technical Secretariat of the GNEJ

Academic Coordinators: Frederico Franco Alvim & Vitor de Andrade Monteiro

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the members of the Board of the Observatory on Social Media, nor of the Electoral Tribunal of the Federal Judiciary of Mexico (TEPJF).

TABLE OF CONTENTS

Prologue

The following comments are the result of a final analysis by the members of the Board of the Observatory on Social Media and are recommended for consideration before reading this document.

The regulatory and judicial overview of the use of artificial intelligence (AI) in electoral processes comes in due time. As more and more elections are influenced by AI, a scientific discussion is needed. This deliverable is not a conclusive work, but a wonderful starting point for ongoing examination.

Currently, there is a significant gap between the expectations surrounding AI and its actual application. Given the rapid evolution of this technology, this report focuses primarily on projections, as it is more useful to explore potential future scenarios, as current ones are often quickly outdated.

AI in the electoral context is a broad and evolving field. It is therefore important to clarify key concepts for readers, such as general AI (AGI), which aims to replicate human tasks, and generative AI (GenAI), which uses existing data to generate new content such as images, videos, and text, among others. This distinction is crucial when discussing issues such as IA bias, the legitimacy of its applications, and where the content comes from. It is important to note that public officials, judges, and civil society representatives often find it difficult to differentiate between these AI models. Moreover, these technologies are not mutually exclusive, as a GenAI application can be part of an AGI.

Future research should address additional risks associated with the use of AI, particularly the capabilities and accuracy attributed to this technology. This includes biometric recognition systems and surveillance technologies, where vendors often misrepresent the accuracy of their tools. Election Management Bodies (EMBs) may also spend too much time on perceived threats such as deepfakes, which have not been a priority concern in recent elections. On the other hand, the increasing presence of embedded AI and augmented reality features into everyday tools deserves attention, as these elements will play an increasingly significant role in resolving electoral disputes.

Overall, this paper seeks to analyze the current landscape and applications of AI in electoral matters worldwide, providing a starting point to guide future research and foster a deeper understanding of this rapidly evolving technology.

1. Introduction

Elections operationalize a specific model of political power legitimization, based on the fact that the exercise of representative functions is conferred to agents who derive the primary source of their authority from the consent of society as a whole (Caretti; De Siervo, 2017). This consent, in turn, directly dialogues with the preservation of a favorable scenario for the realization of free and informed elections, so that popular sovereignty truly acquires an authentic expression.

Initially, the protection of freedom of suffrage and, consequently, the agenda in favor of democratic elections focused on combating violence, fraud, and abuse, presupposing institutional measures against the alteration of official procedures and documents (such as documents, ballots and scrutiny maps), as well as the elimination of behavior related to the abuse of economic and political power (crony, autocratic practices and the like). Over time, in relation to the expansion of the sphere of influence of major media and new technologies, the preservation of autonomy has come to include the need to guarantee equal opportunities in the advertising field, balance and plurality of opinions in journalistic coverage and, more recently, the veracity and integrity of the information environment, security in data management, transparency in computer advertising and the political-partisan neutrality of disruptive technologies.

For some time now, it has been understood that full freedom to vote does not mean the mere absence of direct coercion in the form of bribes, threats or constraints and that other attributes of self-determination need to be preserved, including containing disinformation processes that distort circulating communication (Alvim, 2024), including forms of social engineering based on the exploitation of personal data to apply psychometric pressures and other forms of manipulation that undermine reflection (Han, 2022), decimate analytical capacity (Durand, 2023) and hinder the adoption of a "patient and attentive attitude towards the world" (Sandel, 2022).

As Lozano (2020) observes, the dispersion of attention and the collapse of consciousness lead to "moral consequences" at several levels: the excess of information and the impoverishment of attention trigger an "epistemic distrust" (Ramonet, 2022) that generates not only cognitive consequences but also political (Lozano, 2020) and behavioral (Klein, 2020) consequences, particularly conducive to the fixation of dogmatic thinking and the politics of division. In fact, the lack of rationality diminishes the quality of collective debates, creating a public space receptive to disinformation propaganda, which becomes a permanent feature, both inside and outside official campaigns, to weaken elections (Lissanu;

Moraga; Sobol, 2024), deepen fractures (Kertysova, 2018), attack institutions (Harari, 2024), destabilize governments, demonize opponents, justify forceful measures (Souza Neto, 2020) and reinforce extremist agendas (Vlachos, 2022) and foreign interference campaigns (Gillespie, 2018).[1]

At this juncture, the conscious defense of interests gives way to political behaviors more oriented towards (dis)affective stimuli, leading to "radicalized political polarizations" (Abranches, 2020) that intensify distrust, intransigence, extremism (Slowing-Romero; Scriven, 2024) and the level of conflict in electoral contests (Koffi Annan Foundation, 2020) and in the social landscape itself (Nunes; Traumann, 2023).

This "era of deliberate irrationality" (Levitin, 2019), on the other hand, transforms campaigns into "cognitive wars", making it necessary to adopt measures to preserve electoral normality in addition to the agenda of strengthening integrity, especially with regard to the recovery of its civilized vocation, based on peaceful antagonism as a method of replacing open hostility, mutual aggression, and acute conflict (Alvim; Zilio; Carvalho, 2024). The fact is that new technologies in general, and social media in particular, seem to "reveal the most undesirable aspects of freedom of expression: not informed, productive and reasonable debate on matters of public interest, but disinformation, aggression" (Barcellos; Terra, 2022) and "large-scale radicalization" (Fisher, 2023) on networks.

These dilemmas are not exactly new. On all continents, electoral administration bodies, in one way or another, have been living with disinformation, systematic reputational attacks (Alvim, 2021) and adjacent phenomena—such as hate speech and online intolerance—for almost a decade. However, the rapid expansion of artificial intelligence (AI) tends to resize the horizon of problems, deepening challenges (Bahri et al., 2024) and generating new, robust and unavoidable institutional needs, taking into account that the electoral abuse of intelligent computing poses a real problem, not a hypothetical conjecture (Sapada; Arif, 2024).

Thus, this study addresses the transformations brought about by the progressive incorporation of AI solutions in electoral campaigns, with an emphasis on the impacts of the new political communication on democratic stability and on the microsystem for protecting the normality and integrity of electoral processes. Its reflections are based on the premise that clearly identifying the risks and fully understanding the means by which artificial intelligence operates in the political context are indispensable conditions to reformulate

[1] The crisis of confidence has hit the stability of electoral disputes hard, contributing to the emergence of a veritable epidemic of contested results. According to a major report recently published by IDEA International (2024), in the last two years, in 20% of national elections, at least one defeated candidate or party publicly refused to accept the results, and an identical proportion are decisions that must be decided by the tribunals.

strategies capable of mitigating its negative effects, to guarantee the authenticity of elections and the future of democracy (Yu, 2024).

This paper will aim to analyze the regulatory experiences already developed around the world, as well as the judicial approaches to the use of AI in elections. Finally, recommendations will be presented for a better adaptation and improvement of electoral organizations in the face of the new era of algorithmic elections.

2. Methodologies and Analysis Model

The research uses a combination of techniques, involving a descriptive study applied to define artificial intelligence and map its political uses (positive and negative) and the corresponding impacts on key aspects of electoral governance. From this perspective, the phenomenon researched will be outlined in line with an in-depth review of the available literature, seeking a multidisciplinary approach with doctrinal contributions from technological sciences, Political Science, Social Communication, Ethics of Technology, and various fields of Law (Constitutional, Digital, International, and Electoral).

At the same time, the examination of the case law corpus will be guided by the methodology of judicial decision analysis through the exploratory technique of documentary observation, applying the same method to the research of the normative field. In this area, the aim is to collect a relevant sample of judicial decisions that may exist, to outline an initial "state of the art" (Freitas Filho; Lima, 2010) on the defined object.

The legislative segment, for its part, will be examined, interpreted and classified from ten different perspectives, relating to: i) the scope of the regulatory treatment; ii) the normative rank of the standards; iii) the premise of the regulatory matrix; iv) the general orientation of the initiatives; v) the scope of application of the approved standards; vi) the recipients of the sanctioning standards; vii) the nature and scope of the sanctions provided for; viii) the strata of action covered; ix) the object of protection of the standards that regulate content; and x) the degree of coverage of the risks mapped.

Table 1: Normative corpus analysis dimensions

Dimension of Analysis	Planned Categories
1. Scope of regulatory treatment	a) systematic intervention b) micro-systematic intervention c) timely intervention.

2. Regulatory range of the standards	a) constitutional standards; b) community standards c) legal standards (primary actions) d) infralegal (secondary actions)
3. Premise of the normative matrix	a) risk-based regulation; b) rights-based regulation c) hybrid regulation.
4. General orientation of the initiative	a) permissive regulatory frameworks b) prohibitive regulatory frameworks c) hybrid regulatory frameworks.
5. Scope of the approved standards	a) antitrust standards b) data protection standards c) standards on liability for failure to comply with court orders or for illegal content from third parties; d) standards on the duty of diligence.
6. Recipients of the sanctioning regulations	a) candidates and party organizations; b) social media platforms c) AI developers and solution providers d) content producers and digital influencers e) press media f) politicized people and users in general.
7. Nature of the sanctions provided	a) removal of content; b) imposing of fines c) suspension or banning of profiles, accounts or channels d) disconnection or interruption of the supply of services e) cancellation of the registration of candidates or political mandates f) declaration of ineligibility (disqualification) g) cancellation of elections.
8. Strata of legislative action	a) *the need for authorization to provide electoral services* b) *the business model* (when regulations are approved that condition the marketing of products or services, or that stipulate parameters applicable to the remuneration of content producers); c) *algorithmic programming* (when guidelines or orientations applicable to the calibration of classification, selection and recommendation algorithms are established); d) *social responsibility* (when obligations are established to compensate or restore the information environment in cases of misinformation); e) *behavior control* (when inauthentic actions are prohibited, such as the use of fake profiles, bot agents or mass shooting tools); and e) *content control*
9. Protected legal assets	a) *the freedom to exercise suffrage;* b) *equal opportunities for political competitors*; c) *the honor or image of candidates and parties*; d) *the privacy of Internet users*; e) *the dignity and safety of persons belonging to vulnerable or minority groups;*

	f) *honor, image or trust in guarantee institutions* (tribunals or electoral administration bodies); g) *the peaceful nature of the elections, democratic stability and social peace*
10. Degree of coverage of the mapped risks	(a) *standards against disinformation and inauthentic behavior*; (b) *standards aimed at conflict prevention*; (c) *standards against the manipulation of information flows through algorithms;* (d) *standards against harassment, discrimination and political violence*; (e) *standards against the abusive or irregular use of personal data*; and (f) *standards to preserve the effectiveness of the accountability system based on official controls.*

Source: Compiled by authors.

In terms of **breadth** or scope, disciplinary frameworks will be classified as: a) systematic (when they provide comprehensive treatment to the topic of artificial intelligence, following laws that deal with broader aspects than the electoral process); b) micro-systematic (when they are shaped in electoral reforms that comprehensively deal with AI); or c) specific (when electoral laws deal with isolated aspects of artificial intelligence in a specific, concise and sparse manner).

From the perspective **of the scope of legal intervention**, the standards will be classified according to the origin and nature of the normative process. Thus, the provisions will be classified as: a) *constitutional* (when they update or modify provisions of national constitutions); b) *community-based (*when they come from actions approved by supranational parliaments); c) *legal* (when they are approved by national parliaments and have the rank of primary normative actions); and d) *infralegal* (when they derive directly from decrees of the executive branch or from instructions issued by tribunals or electoral administration bodies legally empowered to do so).

The premise of the regulatory matrix involves a panoramic analysis of the guiding spirit of regulatory solutions. Through this lens, the samples are classified into: a) *risk-based models* (when they are limited to imposing duties and providing for sanctions); b) *rights-based models* (when they mainly establish guarantees for users, stakeholders, and/or the general population); or c) *hybrid models* (when they include prescriptions that fall into both categories).

Based on their **general orientation**, regulatory frameworks will be classified into the following categories: a) *permissive frameworks* (when only standards that clarify the hypotheses in which the use of AI is permitted are identified); b) *prohibitive frameworks* (when only standards that indicate the hypotheses in which the use of AI is prohibited are identified); or c) *hybrid frameworks* (when the confluence of permitted and prohibitive standards is identified).

In regard to the **scope of the approved standards**, it is important to note, for the purposes of highlighting, the option of enacting: a) *antitrust standards* (focusing on competition restrictions or regulations); b) *data protection standards*; c) *standards aimed at holding political actors accountable;* d) *standards aimed at holding big tech companies accountable* (for example, *in cases of non-compliance with court orders or illegal content posted by third parties); e) standards establishing a duty of diligence imposed on developers or providers of AI tools and/or social media platforms*, in cases of non-compliance with court orders or illegal content posted by third parties); e) *standards establishing a duty of diligence* imposed on developers or providers of AI tools and/or social media platforms.

The analysis of the **recipients of the sanctioning regulations** guides the investigation toward the detection and corresponding targeting of the regulations that provide for negative legal responses against: (a) *candidates and partisan entities* (political parties, federations, coalitions or alliances of any kind); (b) *social media platforms* (social networks, microblogs, search engines, private messaging apps, video hosting portals); (c) *developers and providers of artificial intelligence*; (d) *content producers and digital influencers*; (e) *press media* (in physical, analog or digital media); and (f) *politicized people and users in general* (activists, sympathizers, and ordinary individuals).

Regarding the **nature of the sanction**s that may be envisaged, the survey will consider the presence of standards that legitimize the drafting of restrictive administrative or judicial orders, aimed at: a) *removing content*; b) *imposing monetary fines*; c) *suspending or banning profiles, groups or channels on social media*; d) *disconnecting or interrupting the provision of Internet application services*; e) *revoking registrations of candidates or political mandates*; f) *declaring ineligibility or disqualification*; and g) *annulling elections*.

In terms of the **strata of legislative action**, specifically in relation to the operation of social media platforms, the regulations that affect a) *the need for authorization to provide electoral services* (when some type of registration or mandatory measure is foreseen to guarantee the legal operation of the platforms during the electoral period); b) *the business model* (when regulations are approved that condition the commercialization of products or services, or that stipulate parameters applicable to the remuneration of content producers);

c) *algorithmic programming* (when guidelines or orientations applicable to the calibration of classification, selection and recommendation algorithms are established); d) *social responsibility* (when obligations are established to compensate or restore the information environment in cases of disinformation); e) *control of behavior* (when the prohibition of inauthentic actions is established, such as the use of false profiles, bot agents or mass shooting tools); and f) *control of content* (when devices are found to regulate speech or create hypotheses of linguistic abuse).

In regard to the **legal rights protected by content limitation standards**, the provisions located will be classified according to whether they seek to protect: a) *the freedom to vote*; b) *equal opportunities for political competitors*; c) *the honor or image of candidates and parties*; d) *the privacy of Internet users*; e) *the dignity and security of persons belonging to vulnerable or minority groups*; f) *the honor, image or trust in guarantee institutions* (tribunals or electoral administration bodies); or g) *the peaceful nature of elections, democratic stability and social peace*. Given the obvious peculiarities, the standards analyzed here can be classified in more than one way.

Finally, in terms of the **degree of coverage of the mapped risks**, the presence of devices capable of countering the main systemic threats arising from the malicious use of AI in the electoral context will be observed, in particular due to the existence of: (a) stan*dards against disinformation and inauthentic behavior*; (b) *standards aimed at preventing conflicts*; (c) *standards against the manipulation of information flows through algorithm*s; (d) *standards against harassment, discrimination and political violence*; (e) *standards against the abusive or irregular use of personal data*; and (f) *standards to preserve the effectiveness of the accountability system based on official controls.*

Finally, the information collected will be analyzed from a descriptive-prescriptive perspective (Sapada; Arif, 2024), in order to develop a catalog of well-founded recommendations, capable of guiding institutional actions aimed at the institutional defense of electoral integrity against the risks derived from the misuse of new information technologies.

3. Artificial intelligence as a foundational technology and the new order of political communication

Artificial intelligence manifests itself in technological systems or devices capable of reproducing the cognitive capacities of human beings, completing tasks, proposing alternatives or solving problems of varying complexity, through electronic actions based on

learning, reasoning, calculation, creativity or memorization (Degli-Esposti, 2023). When it comes to AI, therefore, we are dealing with "active" computing devices, that is, technological tools that "learn, create on their own and become intuitive", being able to "predict future situations without human intervention and without having to start from scratch with each new situation" (Gabriel, 2022).

In general terms, smart solutions reduce costs, simplify, streamline, improve and, in some cases, automate basic activities and work processes, which makes them integrated into countless governmental, scientific and industrial fronts, as well as gradually assimilating themselves into political and social practices, with important repercussions that affect, among other areas, democratic density (Innerarity, 2024; Kreps; Kriner, 2023) and the effectiveness of national constitutions (Balaguer Callejón, 2023), particularly concerning the defense of public freedoms and other fundamental rights, such as privacy, data protection, equality, free and informed voting (Rubio Núñez; Alvim; Monteiro, 2024), secret suffrage (Mainz; Sønderholm; Uhrenfeldt, 2022) and the concurrence to representative positions under conditions of equity. (Sanchez Muñoz, 2020).[2]

AI applications reorganize public space, promote the reconfiguration of power relations, and are therefore considered more as “sociotechnical means” than mere technological instruments (Pérez de Lama; Sánchez-Laulhé, 2020). Moreover, artificial intelligence can be considered a “foundational technology” as it has unprecedented transformative potential, promising to “reshape our world in ways that are both fascinating and terrifying” (Suleyman; Bhaskar, 2024), given its malleable and dual nature.

Radical transformations, by the way, are already accelerating in the information environment, giving rise to the emergence of a new historical landscape: the era of "algorithmic elections" (Bender, 2022) or the era of "smart elections" (Hammar, 2024), seen as an irreversible, exciting and challenging stage in the competition for citizen votes.

3.1 Artificial Intelligence in Favor of Democracy

In any case, it should be noted that artificial intelligence, despite revealing a worrying set of potential problems, brings with it an equally wide range of positive alternatives (Kertsysova, 2018; Stevenson, 2024), and can be used within the electoral universe for lawful and socially desirable purposes, including as an indispensable strategic asset for

[2] The Degree of Materialization of Democratic Budgets

electoral management bodies to correct historical injustices (Bender, 2022), face present threats and intensify integrity in the future (Rubio Núñez; Alvim; Monteiro, 2024). From this perspective, rather than being understood exclusively as an endless source of problems, smart computing should be seen as an ambivalent emerging phenomenon, certainly fraught with challenges, but equally rich in offering significant opportunities for institutions dedicated to protecting elections (Hammar, 2024; Juneja, 2024; Sapada; Arif, 2024; Suárez, 2024).

In this way, AI simplifies and improves work routines, taking on repetitive tasks, eliminating errors, discovering new methods and reducing economic costs and completion times. In addition, it processes structured and unstructured data to carry out current situation studies, situational calculations, evaluations of sentimental responses and voting patterns, as well as to develop predictive analyses that are now indispensable for effective communication. In addition, the development of natural language makes it possible to automate interactions with the public and drastically reduce the intellectual costs usually required to design informative and persuasive notes. Within this spectrum, artificial intelligence can turbo-charge political campaigns, offering tactical advantages in terms of optimizing the reach and content of messages, gathering information, anticipating results, statistical analysis, segmenting the electorate, and detecting behavioral trends, among other possibilities that are renewed day by day in a spiral that seems infinite (Rubio Núñez; Alvim; Monteiro, 2024).

In schematic terms, AI gives rise to a “paradigm shift” (Safiullah; Parveen, 2021) in electoral contests, as an effect of a host of socio-technical alternatives that can impact, for example, fields such as: a) strategic planning; b) management activities; c) the generation and forwarding of instant responses; d) the adoption of predictive models; e) data collection improvement, categorization and analysis processes; f) the improvement of communication with voters; g) efficiency increase and measurement; h) the opening of communication channels through chatbots and virtual assistants; i) optimization of logistical tasks; j) knowledge of the voter, segmentation of voters and the sending of personalized messages; k) the creation of advertising; l) the monitoring of issues and debates in real time; m) analysis of speeches and sentiments; n) opposition research; o) contrasting campaigns and attacking opponents; p) speech writing; q) public feedback activities; r) cost and expenditure monitoring; s) outcome prediction; t) gathering key information to schedule home visits; u) public image building, legitimizing and polishing; and v) optimizing fundraising and identifying donors (Hammar, 2024; Okoye, 2024; Tomić; Damnjanović; Tomić, 2023; Valdez Zepeda; Aréchiga; Daza Marco, 2024).

Along the same lines, at the institutional level, artificial intelligence is capable of organizing and purifying the electoral census (Chennupati, 2024) and improving the electoral supervision scheme (Stevenson, 2024), both with regard to strengthening security and preventing violence at polling stations (Deepak; Simoes; MacCarthaigh, 2023) and, especially, in the area of combating harmful speech and online disinformation (Kertysova, 2018), as well as optimizing the verification of signatures in documents (e.g. voting by mail) and public petitions (e.g. to support independent candidates or create public parties), and public petitions (e.g. to support independent candidates or create new political parties), the way in which districts are allocated (Bender, 2022) and the mechanisms for controlling and certifying the financial activities of candidates and parties, as well as streamlining the resolution of administrative procedures and court cases, providing greater security, transparency and efficiency in management actions and the adjudication of justice.[3]

Other potential applications by electoral management bodies, in a non-exhaustive list, include statistical modeling techniques for budget forecasting and resource allocation decisions, studies for the rationalization of the distribution (Okoye, 2024), and strategic positioning of polling stations (or tallying centers) (Juneja, 2024), monitoring the programming of radio and television stations regarding compliance with the time allocated to electoral advertising, monitoring enforcement with days of reflection or laws of silence (Bozkurt, 2024), early detection of breakdowns or failures in voting machines and vote to tally counting through video technologies (Deepak; Simoes; MacCarthaigh, 2023), as well as monitoring, organizing and disseminating the origin and sum of financial resources raised or spent on campaign activities, including investments in advertisements or other forms of digital advertising.

AI can also be useful in post-election auditing practices, for example, to detect incidents of fraud. In this way, models developed in advance can provide fact-checked comparisons with actual election results. Furthermore, applications of machine learning and traditional statistics can point out polling stations that show significant differences compared to other polling stations, serving as a starting point for future police or forensic investigations (Juneja, 2024).

Along the same lines, applications based on large language models (LLMs) and, above all, generative AI are particularly useful for enhancing the prebunking and debunking

[3] In this regard, experts comment that AI can be applied to justify the preventive detention of potential criminals, as well as to identify polling stations that, due to key aspects such as a history of crime or altercations, require additional police protection. In addition, smart technologies can recognize vulnerable groups of voters (such as oppressed minorities) whose protection is necessary to ensure the integrity of the process. Finally, AI-based camera systems allow for widespread and scalable automated surveillance that is more effective than human surveillance in detecting fraud or attempted fraud in real time (Deepak; Simoes; MacCarthaigh, 2023).

of fake news, reinforcing fact-checking approaches (including chatbots), saving time and optimizing crisis communication. Other alternatives involve the development of intelligent solutions to detect inauthentic behavior arising from dissemination tools and spam campaigns, as well as “bot-spotting” or “bot-labelling” software used to flag and remove fake accounts operated by trolls or bots (Kertysova, 2018). Artificial intelligence, along the same lines, can be applied to detect the covert use of AI itself in the production of communication content and the manipulation of digital media in general, for example, with the support of tools such as Deep Media, InVID and FakeCatcher (Soon; Quek, 2024). It can also support multi-level citizen education projects, even from an inclusion perspective (Arnold, 2023), for example, with assistive technology resources.[4]

The implementation of intelligent systems "capable of analyzing subtle patterns and inconsistencies in videos and audios can provide a crucial layer of protection against the spread of disinformation". In addition, we can consider the use of Blockchain and Watermarking technologies with the implementation of digital authentication techniques to verify the integrity and origin of audiovisual content" (Tavares, 2024), measures that are more than necessary in the era of second-generation falsehoods. Finally, it is evident that AI can make a solid contribution to the security of electoral systems, detecting potential cyber threats and helping to eliminate external interference in the electoral process (Yazbek, 2024).

It should be noted, as a precaution, that some of these possibilities, while valid and promising, are not without contingencies, which must be duly mapped and weighed, following the internal governance and risk management mechanisms adopted by the electoral management body. The analysis of the pros and cons is already part of academic concerns, as illustrated by a table taken from a research project carried out by researchers at Belfast University:

Table 2: Possibilities, Potential Risks and Avenues for the Use of AI in Key Aspects:

Avenue	AI Use	Risks	Paths
Voter List Management	Approaches by heuristic approaches Linking records Outlier detection	Balancing issues between access and integrity AI biases AI overgeneralization	Access-focused AI Reasonable explanations Local control

[4]AI can be used by electoral bodies in more trivial actions, such as the immediate translation of meetings, classes or conferences into a foreign language, facilitating the exchange of experiences and knowledge between allied organizations, among many other possible applications.

Location of voting stations	Determining the location of mailboxes Location of facilities Grouping	Organizational ethics Volatility and search costs Partisan manipulation	Plural results AI Audit Disadvantaged voters
Predicting problematic stations	Predictive surveillance Design of historical series	Systemic racism Aggravated brutality Feedback loops	Transparency Statistical rigor Fair AI
Voter authentication	Facial recognition Biometrics	Race or gender biases Unknown biases Stake Surveillance and others	Alternatives Bias audit Design for extreme cases
Video monitoring	Video vote recount Event Detection Re-identification of persons	Electoral Integrity Marginalized communities Weakening of other controls	Surface monitoring Open data

Source: Deepak; Simoes; MacCarthaigh, 2023

Based on surveys conducted by researchers from various countries, we have compiled a non-exhaustive catalogue of smart solutions already implemented by governments and electoral administration bodies in various countries around the world:

- **Argentina:** In June of this year, the province of Corrientes carried out a pilot project on artificial intelligence with the reading of documents using sequenced neural networks (transformer technology) (Suárez, 2024), which was successful in optimizing and speeding up the process of transmission and recounting of votes.
- **Brazil (nationwide):** The country has been using an AI-based facial recognition system for over a decade. This technique allows for biometric identification in the voting eligibility process, and also serves to prevent fraud in cases of duplicate, multiple or usurped identities in the electoral census. Along the same lines, the use of AI-synthesized voice has been implemented to help visually impaired people vote at electronic ballot boxes, which will be used starting with the 2024 municipal elections. The Superior Electoral Tribunal (TSE by its Portuguese acronym) also created a chatbot for voter services in collaboration with WhatsApp, which was also used to debunk rumors and disinformation narratives. By including an opt-in feature, the chatbot sent proactive alerts on important topics with consent. With over 6.2 million active users and some 20 million messages exchanged, the chatbot has become one of the largest on the platform worldwide. In addition, the TSE, through strategic partnerships, has the support of network observatories and companies that monitor open data on social networks, periodically providing information and analysis reports on the circulation of the main disinformation narratives.
- **Brazil (subnational level):** In the country, some regional electoral tribunals (TREs by their Spanish acronym) have developed AI solutions for various purposes. The Janus system—developed by the TRE of Bahia and subsequently adopted by many other tribunals in the country—is a procedural automation solution capable of increasing productivity and efficiency in the delivery of justice, streamlining the evaluation of low-complexity cases, for example, in matters of candidate registration and accountability of electoral campaigns. In addition, the Bahian tribunal offers students and interested public an immersive visit through a virtual reality-based experience (including the possibility of using 3D glasses). The TRE of Pernambuco, on another front, has developed a bot to monitor posts, evaluate content and responses in order to monitor the disinformation landscape on social network X during the 2022 elections. Another project of this tribunal included a tool that uses AI and bots to facilitate the audit process of the operation of electronic ballot boxes, with a view to increasing citizen confidence. Ahead of the 2024 municipal elections, the TRE of Goiás launched GuaIA,

a tool for analyzing publications on websites and media outlets, as well as audio and video clips containing distorted or misleading news about the electoral process. Since 2022, the TRE of Paraíba has been applying AI to a Remote Voter Assistance System and, in the middle of this year, it launched a pioneering intelligent system (uIAra), which calculates the probability that audio media are deepfakes. Also in 2024, the TRE of Maranhão launched a virtual assistant that uses artificial intelligence to generate *ementas* (summaries of judgments) for collegiate judicial decisions issued by the tribunal.[5]

- **Canada:** Election management bodies have been exploring AI applications to improve election accessibility, including developing chatbots to provide inclusive information to all voters (Yazbek, 2024).
- **Colombia:** The National Civil Registry uses smart tools in electoral and voter identification processes. In addition, a model focused on pre-electoral logistics is being developed, capable of providing early alerts so that officials can identify circumstances that merit attention during all organizational stages (Penagos Ramírez, 2024).
- **South Korea:** In the 2020 parliamentary elections, an AI model was used to count votes. The technology was able to reduce recounting time and mitigate human error by properly examining votes using machine learning techniques. This integration substantially improved the overall effectiveness of the electoral process (Chennupati, 2024).
- **United States:** To make voting more manageable and accessible, the country has been investigating the use of AI in voting systems. West Virginia is a good example: in 2018, the state launched a test program to allow foreign service members to vote through Voatz, a mobile voting software. To ensure that votes are secure and legitimate, the app employs AI algorithms and blockchain technology, using biometric data and facial recognition technology to provide an accurate identification of each voter (Chennupati, 2024). Furthermore, in regions such as Kansas and the District of Columbia, cross-checking algorithms have supported experimental voter registration purge programs designed to remove instances of voters improperly registered in two or more states across the Union. What's more, at least 29 counties in eight different states have used signature verification programs, mostly to validate or invalidate mail-in votes (Bender, 2022; Juneja, 2024).
- **Estonia:** The country has been using AI in voting systems since 2005, reinforcing its reputation for being at the forefront of e-government projects. One example is the implementation of the i-voting system, which allows anyone to vote online securely. In this context, AI algorithms play a crucial role in ensuring the honesty of the voting process (Chennupati, 2024; Deepak; Simoes; MacCarthaigh, 2023).
- **India:** The Indian government has been exploring AI to improve election security, including detecting fake news and identifying suspicious digital activities during the election period (Yazbek, 2024). In parallel, voter facial recognition systems have been tested in some contexts since the 2020 Telangana municipal elections. Also, in the 2021 Bahir state elections, authorities tested video analytics technology to check the accuracy of manually counted votes (Deepak; Simoes; MacCarthaigh, 2023).
- **Indonesia:** Powered by AI, the Voter List Information System (Sidalih) has been in place since 2014 to help the General Election Commission (KPU by its Indonesian acronym) build up an honest voter base, increasing the reliability of public consultations (Akbar et al., 2021).
- **Libya:** With support from the United Nations Development Programme (UNDP), the High National Electoral Commission (HNEC) held a training workshop on monitoring online violence against women in elections, using AI tools to collect quantifiable data to monitor and

[5] Between September 2022 and February 2023, the AletheIA tool identified more than 1.9 million disinformation messages against the Brazilian elections on X. Combining AI and advanced data analysis techniques, the model collects open data from social media based on hashtags and keywords, processing the texts to eliminate irrelevant information. It also classifies the texts, grouping them by sentiment (positive or negative) to help identify disinformation. The system is also able to automatically send official information to editors, with valid explanations of topics previously categorized as inappropriate.

understand the causes of harassment and digital gender-based violence, in order to guide the search for solutions (UNDP, 2022).

- **Mexico:** The National Electoral Institute (INE by its Spanish acronym) has developed a text recognition tool, which will be used from 2024 for reading documents and recounting votes in order to speed up the publication of preliminary results of the electoral processes (Riquelme, 2023). At the same time, the Electoral Tribunal of the Federal Judiciary (TEPJF by its Spanish acronym) is developing an AI civic service to help candidates, political parties and citizens in general to find the best way (administrative or judicial) to assert their rights before the electoral justice system (López Ponce, 2024).
- **Nigeria:** The Independent National Electoral Commission (INEC) has launched a pilot project for the gradual introduction of AI into its operations. The INEC Voter Enrolment Device (IVED) and Bimodal Accreditation System (BVAS) improve the quality of data capture in voter registration by applying a bimodal technology that brings together fingerprints and facial prints, replacing the initial model that focused solely on fingerprints. Within the Commission, the Automated Biometric Identification System also uses AI elements in its operations (Okoye, 2024).
- **Kenya:** Starting in 2017, a smart biometric identification system was implemented that uses computer vision and fingerprint scanning to verify voter identity and prevent electoral fraud (Carter Center, 2022; Yazbek, 2024). Similarly, with support from the International Foundation for Electoral Systems (IFES), the Independent Electoral Borders Commission (IEBC) implemented a custom smart tool that provided a platform to detect, record, and analyze hate speech on X. Throughout the electoral cycle, the tool enabled the commission to better manage factual inconsistencies, identify potential security risks, and train its staff in monitoring media at the National Recounting Center (Kolb, 2022).[6]
- **Switzerland:** The country is also at the forefront of technology, experimenting with new voting techniques based on blockchain and artificial intelligence. In 2018, the city of Zug piloted a blockchain system in municipal elections, allowing voting via mobile devices. AI algorithms will increase the accuracy of voter identification and reduce the possibility of fraud, while blockchain technology has enabled a transparent, secure and immutable voting process (Chennupati, 2024).

New technologies can also reinforce the participatory and monitoring functions performed by citizens and civil society, for example, by facilitating the organization of collective interests (through manifestos, petitions and other forms of demand), improving the accessibility to voting (Juneja, 2024) and communication elements, organizing the excess of current information, for example, through apps that systematize and compare the judicial history, political platforms and sources of financing of different candidates, and by creating tools for detecting and monitoring inauthentic behavior and the circulation of hate

[6] Throughout the implementation of this system, it was discovered that approximately 1.2 million deceased voters were still listed on the Electoral Roll (Mosero, 2022), opening up room for voting fraud.

speech and digital disinformation on the internet, through social listening tools that flag or even anticipate cases of viral impact (Kertysova, 2018).[789101112]

They can also allow for the automated production of journalistic stories of public interest, to fill the information deficit of people living in remote regions affected by information vacuum or news deserts (Aramburú Moncada; López Redondo; López Hidalgo, 2023), as well as facilitating, through “gamification” applications (with questionnaire tools), the comparison between the values honored by voters and the platforms of competing alternatives (Machado; Portella, 2024). In addition, artificial intelligence makes it possible to independently check the scrutiny and counting data, including through electoral observation missions (Yazbek, 2024), as well as helping people with questions, for example, about polling stations or the documentation necessary to exercise their civic duties, through virtual assistance models with natural language processing.[1314]

Therefore, in general terms, AI solutions can reduce the possibility of fraud, deter malicious actors from acting, and protect democratic integrity by enabling proactive, timely, and accurate reactions to prevent, eliminate, or punish certain anomalies in key aspects of election organization (Chennupati, 2024; Stevenson, 2024).[15]

---

[7] The same reasoning applies to auxiliary bodies of justice, such as the Public Prosecutor's Office in Brazil. Along these lines, the Public Prosecutor's Office of Rio de Janeiro in 2024 used AI to speed up the process of evaluating and eventually challenging irregular candidacies.

[8] In Israel, OrCam Technologies has developed the MyEye 2.0 device, which increases the autonomy of visually impaired people. The device has been used in the country to enable voters in this segment to cast their ballots without any assistance (Suárez, 2024).

[9] In Switzerland, the Alliance F project has developed an algorithm called Bot Dog, responsible for the proactive and automated detection of hate messages (Suárez, 2024).

[10] "AI has contributed substantially to electoral accessibility by creating alternative voting procedures that accommodate the needs of people with disabilities or mobility issues. People can use accessible interfaces, such as screen readers or voice commands, to vote remotely through AI-powered e-voting systems, allowing people to vote from the comfort of their homes. In addition to removing physical barriers to voting, these solutions ensure the privacy and security of voters with visual impairments or other disabilities. AI-powered voice interfaces have emerged as another transformative tool to improve accessibility in electoral processes. These interfaces enable voters with motor or speech disabilities to interact with voting systems using natural language commands or audio instructions, facilitating independent and dignified participation in the electoral process. By removing language and literacy barriers, voice interfaces enable people with diverse abilities to exercise their right to vote without assistance or discrimination." (Stevenson, 2024).

[11] La aplicación "Voto Legal", desarrollada por el Movimiento de Combate a la Corrupción Electoral (MCCE) y la iniciativa App Cívico en Brasil, es un buen ejemplo. Con el objetivo de promover unas elecciones más justas y transparentes, la solución utilizaba registros blockchain y una interfaz con un lenguaje claro sobre las propuestas políticas, con el fin de ayudar a tomar decisiones informadas. Available at: [https://www.appcivico.com/historias-de-sucesso/voto-legal]. Accessed: 02.09.2024.

[12] In Spain, for example, the company Chocolate designed Elecciones.chat, a chatbot and voicebot available for voice assistants such as Alexa, as well as WhatsApp, through which users can learn about the different government platforms while doing household chores (Suárez, 2024).

[13] In Brazil, the Superior Electoral Tribunal launched a chatbot in collaboration with WhatsApp in 2020. In 2022, the solution, which had also been reworked to debunk disinformation, was used by more than 6.2 million voters, allowing the exchange of more than 177 million messages. It has thus become one of the largest chatbots on the platform worldwide (Tribunal Superior Eleitoral, 2023).

[14] A platform created by the State University of Campinas (Unicamp) in collaboration with the State University of Rio de Janeiro (UERJ) uses AI to compare more than 60,000 government programs presented in municipal elections in Brazil. With the tool, users can search and compare proposals on the issues that interest them most, without having to review the complete proposals of all the candidates (Soares, 2024).

[15] To this end, there are tools capable of exercising preventive moderation, acting to eliminate harmful content even before it is published. Some examples are automated image recognition tools with hash technology, such as PhotoDNA, created

It is important to note, within this reasoning, that fraud, abuse, and manipulation exist, but they are not the only or the most prominent forms of exploiting artificial intelligence in the context of elections (Jungherr; Rauchfleisch; Wuttke, 2023). This understanding is essential so that governments and electoral institutions do not consolidate a limited and refractory understanding that discourages the necessary investment in innovations that can be exploited.

Graphically, the following table compiles a diverse (and non-exhaustive) set of positive uses of AI in electoral processes, as observed around the world. Each possibility contributes to some purpose related to the integrity of the process (inclusion of vulnerable segments, reduction of economic costs, purging illegal or antisocial practices, raising the ethical level of competition, and facilitating the right to access information).[16]

by Microsoft, which helps detect child pornography material in advance, and ContentID, from Youtube, which exhaustively scans the system, finding and eliminating videos with copyright infringements (Fux; Fonseca, 2022).

[16] Kumar Chennupati (2024) advierte que: "las consideraciones de accesibilidad e inclusión deben preceder al uso de la IA en las elecciones. Algunos programas informatizados pueden excluir a personas por falta de alfabetización digital o de acceso a la tecnología. Para garantizar que todo el mundo tenga las mismas oportunidades de votar, debemos dar cabida a las personas que decidan no utilizar o no puedan manejar dispositivos informáticos. Las personas que ya están en desventaja, como los hablantes no nativos o las comunidades desfavorecidas, pueden verse aún más afectadas si los sistemas de IA perpetúan deliberadamente estereotipos culturales o lingüísticos". Por eso, entre otros factores, "es esencial tener en cuenta la diversidad artística y lingüística para garantizar un acceso y una comprensión equitativos".

Table 3: Legitimate Applications of AI in Electoral Campaigns

• Realistic voice-over automation • (inclusion)	• Automatic generation of subtitles and optional captions • (inclusion)	• Voice and image biometrics to debunk deepfakes • (debugging)	• Automated detection of disinformation and harmful content • (debugging)
• Automatic detection of unwanted content (criticism, rumours and negative propaganda) • (competitiveness)	• Monitoring news coverage (clipping) to detect negative stories • (competitiveness)	• Monitoring public groups in messaging applications, with semantic treatment of impact indicators (trend and sentiment analysis) • (competitiveness)	• Comprehensive assistance or development of campaign platforms • (competitiveness)
• Monitoring the legality of opposing campaigns, including the detection of inauthentic behavior • (debugging)	• Monitoring and analyzing the digital performance of agendas and the evolution of competitors • (competitiveness)	• Predictive models for tactical optimization (profiling of undecided voters, anticipation of influential topics) • (competitiveness)	• Prescriptive models for (re)orientation of approaches (georeferencing of rejection hotspots, neurolinguistic recommendation software) • (competitiveness)
• Automated management of profiles, groups and channels on social networks (post scheduling) • (economy)	• Chatbots for voter service (Ask questions, collect data, detail proposals, encourage participation, present fact-checking materials). • (competitiveness)	• Data mining for lawful purposes • (competitiveness)	• Personalization of lawful advertising • (competitiveness)
• Synthetic production of positive advertising (jingles, slogans, cards, etc.) • (economy)	• Synthetic production of materials	• Information/propositional documents (writing statements, briefings for debates, texts for the right of reply) • (competitiveness)	• Call center automation • (economy)
• Editing, correcting or improving audio, video or image content • (economy)	• Self-detection systems to reveal irregular use of generative AI by adversaries • (debugging)	• Virtual assistants for the organization of bureaucratic tasks (payment scheduling, accounting legality control) • (economy)	• Civic applications to organize information and compare competing alternatives • (right to (information)
	• Synthesis systems to facilitate the understanding of political information • (right to information)		

Source: Rubio Núñez; Alvim; Monteiro (2024), with additions and adaptations.

3.2 Artificial Intelligence Against Democracy

However, it is clear that, on the negative side, the technological revolution is reshaping the landscape of political communication, the media industry, the nature of the market of ideas and the pattern of information consumption. As a result, the landscape of vote-seeking, the organization of collective interests, public behavior, and the dynamics of building (and deconstructing) social trust have been realigned in clearly detrimental ways. The most radical innovations concern, on the one hand, the progressive incorporation of algorithms by information retrieval platforms (search engines) and social media and, on the other, the accelerated expansion of natural language processing and generative artificial intelligence (GAI) systems, adept at creating shortcuts to the production of inaccurate information.

Furthermore, these elements radically alter the ecosystem of information production, introduce new actors into public discussions, empower malicious groups, and jeopardize the hierarchical order of source credibility (Kavanagh; Rich, 2018), giving rise to an inflated, superficial, intolerant and hostile digital sphere, in which opinions are confused with facts (Charaudeau, 2016). Within this scenario, narratives challenge objective reality, technology creates evidence for false claims (Filimowicz, 2022) and people, paradoxically, “no longer believe in nothing and, at the same time, are capable of believing in anything” (Grijelmo, 2017).

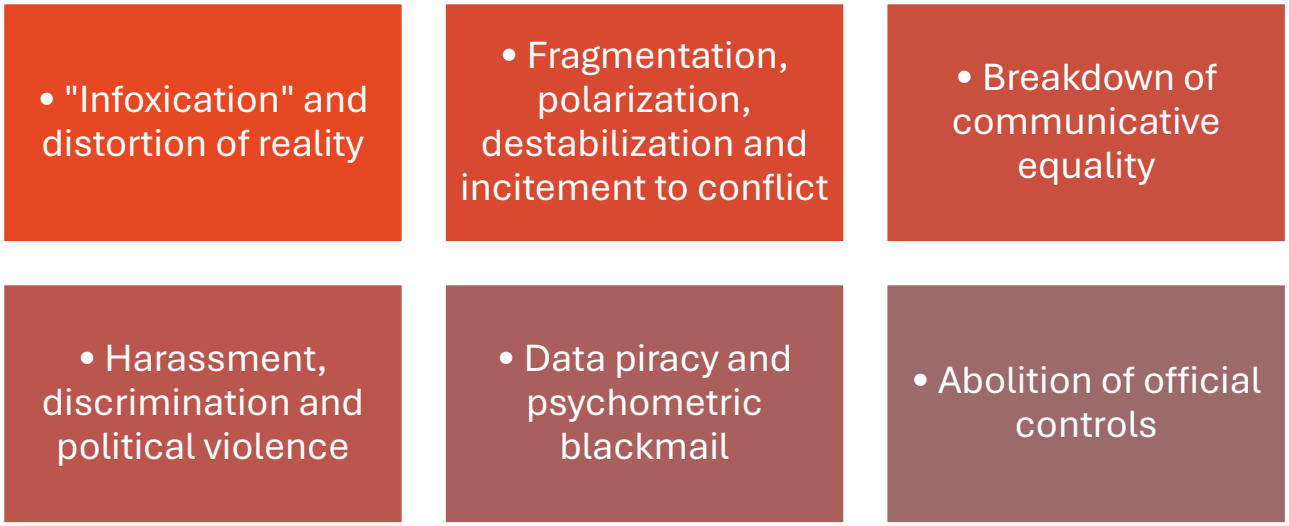
These issues greatly increase the availability, receptivity, and modes of production, distribution, and exchange of “corrosive discourses” (Zachary, 2020), including the advocacy of anti-democratic agendas and disinformation narratives.

The landscape shows that AI makes it easy for anyone to create and spread harmful content, making it “a particularly dangerous tool for democracy when used in bad faith” (Denemark, 2024). Disinformation generated by artificial intelligence, in particular, was recently classified in a World Economic Forum report as the “top emerging risk” in the next two years (World Economic Forum, 2024), and the incredibly rapid advancement of this technology suggests that the landscape of harmful activities is often renewed, going beyond the mere sophistication of old, well-known disorders (Hawes; Hall; Ryan, 2023).

Considering their direct and indirect effects, Rafael Rubio, Frederico Alvim and Vitor Monteiro (2024) believe that, in the context of electoral campaigns, smart solutions instrumentalize a wide range of undesirable behaviors capable of undermining the framework of basic rights and freedoms for honest, fair and free elections. These behaviors

have been systematized in different categories that, together, make up a taxonomic model segmented into six fronts:

Image 1: Taxonomy of AI-based information disorders



Source: Rubio Núñez; Alvim; Monteiro (2024).

The related practices will then be analyzed, taking the aforementioned theoretical framework as a central reference.

A. “Infoxication” and distortion of reality

Reality-altering practices involve the automation of processes and the mass distribution of fake news, cheapfakes, deepfakes, rumors, and other false narratives, as well as the creation of false opinion movements in virtual communities (astroturfing), based mainly on inauthentic behavior carried out by bots that disrupt and influence sensitive social processes. At the same time, artificial intelligence can obstruct access to important issues and the reality of the facts by overloading information through mass dissemination tools (spreaders, spambots) and automated accounts used to spread distractions (smokescreens) or intensive disinformation campaigns (firehosing). In addition, AI

hallucinations, even if accidental, can significantly damage the information landscape, jeopardizing elections (Rubio Núñez; Alvim; Monteiro, 2024).[17]

As evidence of IAGen's clear potential to carry out covert interference campaigns, OpenAI recently revealed the discovery of malicious use of its platform in five destabilization operations systematically carried out by foreign actors. Using the ChatGPT tool to generate and translate news articles and short comments that fed fake accounts, the operators of the scheme sought to influence public debates around certain agendas on social media (Carrascón, 2024).[18]

B. Fragmentation, Polarization, Destabilization and Incitement to Conflict

From this perspective, the same tools used to produce disinformation can be used to design, publish, and make other types of harmful discourse go viral, used as a lever to mobilize segments of the population that feel deceived, betrayed or excluded. From this point of view, artificial intelligence fuels the political exploitation of hatred and mistrust, reinforcing aggressive and intolerant behavior against minority or vulnerable groups, and opposing ideological currents or electoral institutions. Alongside misleading narratives, therefore, intelligent solutions can be mobilized to spread extremist and radical content, with strong negative repercussions on the electoral process (Rubio Núñez; Alvim; Monteiro, 2024).

Social media algorithms, in particular, are largely responsible for the "heyday of polarization" (Vivas Escribano, 2023), which often takes place in echo chambers that reinforce, feedback and enhance negative antipathies, animosities, and prejudices that induce strong social divisions. According to various studies, virtual communities crystallize identities and create barriers between political groups, facilitate ideological hyper-emotionality and, consequently, deepen political and sentimental fractures, stimulating the circulation of messages that evoke feelings of anger and disgust (López-Ponce; Barredo-

[17] Hallucinations occur when generative AI models, due to some fault, create answers or annotations that appear reliable, but are false (Panditharatne; Giansiracusa, 2023). For example, research carried out by the AI Democracy Projects organization involving five different chatbot models concluded that queries on electoral issues returned false or inaccurate results in 50% of attempts (Soon; Quek, 2024).

[18] The five operations detected included a) a Russian operation targeting Ukraine, the Baltic states, and the United States, focused on creating politically motivated comments for distribution on the Telegram app ("Operation Bad Grammar"); b) a Russian effort to produce comments in multiple languages, using platforms such as X and 9GAG for dissemination ("Operation Double"); c) a Chinese network using AI to create multilingual texts and manage online platforms (Operation "Spam Camouflage"); d) an Iranian scheme producing and translating long-form articles for publication on affiliated websites (Operation "International Union of Virtual Media" — IUVM); and e) an Israeli commercial enterprise creating articles and comments for social media platforms such as Instagram, X, and Facebook (Operation "Zero Zeno") (Matoruga, 2024).

Ibáñez; Sánchez Gonzales, 2024) with highly contagious effects among the population (Martinez-Brawley, 2024).

C. Violation of Communicative Equality

On social media, artificial intelligence, in combination with other digital technologies (such as mass-shot techniques), shapes the general framework of ideas and opinions that will reach each user, designing the window through which users view the world. Since they select everything that will be seen or ignored—and how strongly each message will circulate—content prioritization and recommendation algorithms play an important role in the formation of beliefs and the consolidation of electoral options (Rubio Núñez; Alvim; Monteiro, 2024).

At the same time, automated content moderation also affects the overall landscape of online communication, which can lead to the systematic removal or reduction of the scope of certain topics, the reduction of the credibility of certain claims (with the insertion of labels, flags or warning screens, pointing out the existence of false or dubious content, for example) and, ultimately, to the exclusion of speakers or discussion groups, as a result of suspension or ban decisions for the alleged violation, repeated or not, of community standards or related policies (Oliva; Tavares; Valente, 2020). Although massive learning algorithms exist, at least in theory, to recognize problematic content free of human bias (Gillespie, 2018), the truth is that computational techniques make decisions with strong socio-political implications.

The presence of inaccuracies or biases in tools based on large language models (LLM) can also affect the quality of the information landscape, generating distortions that impact the political dimension of public opinion. The provision of biased or incorrect answers by generative solutions creates additional challenges in terms of eliminating systems of privilege, which can favor certain ideological inclinations to the detriment of others (Rotaru; Anagnoste; Oancea, 2024), affecting the expected balance between the poles.

In light of the above, demanding partisan neutrality on digital platforms becomes important, given that the main space for the development of politics today is dominated by large technology companies that, by imposing terms and conditions, gain the ability to apply private guidelines to the "judgment" of specific cases and exercise "quasi-legislative", "quasi-judicial" (Fux; Fonseca, 2022) and "quasi-governmental" powers (Cupać; Schopmans; Tuncer-Ebertürk, 2024), with serious consequences for electoral competition.

D. Harassment, Discrimination and Political Violence

Just as networks connect people who know and like each other, or who share similar beliefs and tastes, they also bring together individuals and groups who think and have different opinions, whether on minor, initially trivial issues, or on sensitive, controversial and highly relevant aspects. In this context, just as virtual communities host users who are understanding, tolerant and cordial with dissonance, they also host legions of intolerant, provocative and uncivilized individuals, antidemocratic and antisocial affections and practices, expressed in different forms of discrimination, harassment and political violence (Rubio Núñez; Alvim; Monteiro, 2024), often stimulated by a pernicious scheme of gratification, materialized in digital applause found in emojis, social buttons or visceral comments of encouragement.

In this environment, there is concern about a “systematic displacement of communication boundaries, especially to the detriment of vulnerable groups whose [political and] personality rights are threatened”, as well as the fact that these demonstrations endanger “the fundamental standards of an open discourse of free and equal citizens in a democratic society” (Eifert, 2022). The exposed minorities are, at the same time, perpetual victims of hostile persecution and the single-issue object of manipulative tactics that lower their dignity through inventions, exaggerations and generalizations, managed to manipulate the opinion of outgroups through fanciful narratives of existential threats, oxygen for the culture of hate and the politics of fear.

The recurring incidence of trolling produces a normalizing effect on illegitimate discourses, which, through unrepressed repetition, end up gaining a captive reserve in discussion spaces, as a result of a communication phenomenon known as the "Overton window." Through recurrence, abundance, and tacit (and sometimes explicit) acceptance, identity attacks are (re)installed in the social landscape, as if they were part of it, as if through some distorted vision of the law (the scarecrow created by the libertarian absolutism of expression) they could remain there.

E. Data Piracy and Psychometric Blackmail

The digitalization of business, commercial transactions, the circulation of information, public services and human interactions in individual and collective terms has transported an enormous amount of data to the dimension of the network, establishing the raw material necessary for algorithms to decode the gears of the world and come into play as a business

model that revolutionizes the dimensions of electoral advertising (Rubio Núñez; Alvim; Monteiro, 2024).

Big data models help candidates, political parties, and malicious actors read voters' minds and see patterns of behavior, invisible correlations, and other insights with incredible clarity (Safiullah; Parveen, 2021). Under these conditions, propaganda becomes much more effective and precise, reaching the right people at the right time (Hawes; Hall; Ryan, 2023), given the ability to detect moments of vulnerability or increased personal or group susceptibility (Tavares, 2022).

F. Abolition of Official Controls

Due to its characteristics, network architecture relies on economy, ubiquity, ease of access, speed and, above all, the lack of prior control and anonymity to bring together a huge set of users given to harmful behaviors and practices that violate fundamental rights (Herrerías Castro, 2023). AI also plays a role in these issues, since intelligent computing enables remote cyberattacks, in addition to providing solutions that weaken the accountability system by adding layers of impunity and anonymity (Rubio Núñez; Alvim; Monteiro, 2024), in addition to the fact that many of the dysfunctions discussed tend to occur silently and surreptitiously, if not invisibly. The risks, from this perspective, end up expanding due to the disproportionate relationship between the amount of the prize and the possible inconveniences for the subjects in action (Vacarelu, 2023).

What's more, malicious actors investing in AI to exploit disinformation are "highly adaptable, continually refining their strategies to avoid detection." As platforms deploy new defenses and identification technologies, these actors find new vulnerabilities to exploit, or develop even more sophisticated intelligent models to bypass filters. This "continuous cat-and-mouse game" represents a significant challenge in the search for effective and lasting solutions capable of effectively mitigating harmful AI-driven content (Yu, 2024).

4. Premises for Understanding the Regulatory Debate

In general terms, the concept of regulation encompasses the idea of ordering economic activities to ensure that these activities are carried out in harmony with certain social objectives, beyond the strict interests of the respective market. Although regulation has traditionally been understood as an agreement on economic activities, the notion is also

applied to the context of social regulation, understood as an intervention that does not have the regulation of a market as its immediate objective, but rather the regulation of aspects of the behavior of subjects that operate in a certain legal area and that are relevant from a collective perspective. From this angle, the treatment of social networks and their algorithms implies a regulatory debate, given that these networks centralize an advertising market and an information traffic market, as well as the market for exchanges and interaction between users (Farinho, 2022).

Although the Internet is usually made up of different layers—a) the infrastructure layer; b) the code layer; c) the application layer; and d) the content layer, according to Lessig's seminal definition (1999)—the truth is that, in its intersections with electoral matters, regulatory claims tend to focus on the last two. Within this area, established standards generally tend to ignore considerations regarding equipment and infrastructure assumptions, such as fiber optic cables, as well as details related to the interoperability of networks and connection and navigation protocols, to focus on aspects related to the governance and operation of digital platforms, as well as the set of publications they receive, make available and use.

The latest electoral cycles demonstrate that "the rise of artificial intelligence has changed the conditions under which society communicates and generates knowledge", bringing novelties that both challenge and demand a normative movement with institutional responses (Vesting, 2022). The normative concern in this segment tends to prevent the "control of the standards of the game" provided by digital technologies from descending to an exacerbated "degree of alienation" from the values and guiding principles of law (Tavares, 2022), to ensure that electoral contests absorb technological transformations while maintaining their democratic essence. In other words, to ensure that new technologies conform to democratic standards, and not that democracy submits to the business model of new technologies.

Despite sharing a common goal, the truth is that the different legal systems do not necessarily follow the same path, given not only the weight of the differences related to historical tradition and legal culture, as well as the pressures and contingencies that affect the political and social climate and will, but (also) the almost simultaneous emergence of a varied arsenal of possible approaches that adds a layer of complexity (Bozkurt, 2024) to the already arduous task of choosing. As an example, the current state of the art offers interested authorities and governments the possibility of investing, alternatively a) in declarations of principles and ethical standards; b) in the adaptation of existing regulations, trying to adapt them to the context of AI and proposing new ways of addressing the specific

challenges of the technology; c) in the design of government strategies for the regulation of AI, including the creation of regulatory agencies, the implementation of public policies and the promotion of responsible research and development; and d) the creation of structured models that guide the development, implementation and use of AI, combining ethical principles with practical recommendations and governance mechanisms based on frameworks and guidelines (Almeida; Santos; Farias, 2021).

As for the substantive issues, the normative content will depend on "choices made on the basis of political and social deliberations intertwined with the culture, historical development and the law of each sovereign nation" (Fux; Fonseca, 2022), especially with regard to the different views on the dichotomy of freedom of expression versus protection of the integrity or legitimacy of elections, which, for these purposes, transfers the old discussions on the (weak or powerful) role of the State in guiding society to the dimension of network governance (Fachin; Veronese, 2024).

In this context, the split between libertarian and protectionist systems, together with the different degrees of risk and exposure to anti-democratic, protest, and coup practices, gives rise to the emergence of more contained systems (minimalist models) on the one hand and more complete systems (maximalist models) on the other, endowed with a greater sense of intervention as a result of a tacit commitment to a notion of substantive democracy, combined with the idea of militant democracy. These same circumstances also make it "natural and expected" that occasional "frictions" occur between global technologies and some local regulations (Estarque; Archegas, 2021).[19]

Understanding the importance of AI in elections requires being aware of the many views and issues that exist across countries and locations. Technologically mature nations tend to have a more nuanced understanding of the dangers of AI (Chennupati, 2024), which

[19] From this perspective, it is worth recalling "[...] the different weight given to freedom of expression in the various models of democracy. The term is used to describe a variety of models of state organization and it is therefore possible to identify different axes along which models of democracy vary. Two of them deserve to be highlighted [...] for their influence on the role attributed to freedom of expression. The first classifies democracies as substantive or procedural. The latter are concerned with guaranteeing formal democratic procedures, such as periodic and free elections, without entering into qualitative considerations about the results of these procedures. Substantive democracies, on the other hand, are concerned not only with formal procedures, but also with the results produced. Considerations such as guaranteeing the material equality of all groups are therefore important. In this context, procedural democracies tend to value freedom of expression for its own sake, based on the perception that it is essential for the subsistence and legitimacy of formal democratic procedures. Substantive democracies, on the other hand, tend to allow for greater state interference in speech, with the goal of promoting specific substantive outcomes. [...] The second axis involves the gradation between libertarian and militant democracies. The main element that distinguishes these categories is the freedom granted to speech and to organizations that oppose and threaten the very democratic structures that make self-government possible. On the one hand, libertarian democracies grant strong protections to this kind of speech as well, allowing regulation only from the point at which the speech becomes an imminent threat of political violence. [...] On the other hand, militant democracies allow restrictions on speech or on the existence of groups (e.g., political parties) that attack democratic institutions, even when there is no imminent risk of political violence. And this is not only to protect democracies from possible violent attacks, but also to protect them from the possibility of subversion by democratic means, as occurred, for example, with the rise of the Nazi party in Germany in 1933, elected by a legitimate electoral process" (Barroso, 2023).

tends to be reflected in a greater ability to regulate technologies based on independent, situation-appropriate thinking. Meanwhile, in less developed environments, less knowledge encourages outright importation of foreign models.

The major problem is that, in the field of electoral reforms, the effects of the devices necessarily vary depending on the socio-political conditions of the environment in which they are applied. From this perspective, the apparent success of a model in a given place does not guarantee absolute success on the national stage, since experience shows that identical models often have different results in different countries (Meirinho Martins, 2015). When it comes to electoral systems, the context makes the difference (Nohlen, 2015), so that the same provision can, logically, have radically different political effects when applied in different environments. Hence the conclusion that the importation of foreign models must be preceded by a thorough diagnosis of the country's economic situation.

5. Case Studies on Regulatory Experiences with AI in Elections

The regulatory framework for the use of AI in electoral processes is still quite incipient, proving limited and timid in the face of the immense challenges posed by these technologies. Although several international institutions have already worked to create democratic protection frameworks adapted to this new context, electoral regulation continues to depend largely on the self-regulatory initiative of technology providers, which experience has shown to be quite insufficient (Rubio Núñez; Alvim; Monteiro, 2024).

In this sense, it is essential to create an institutional framework that regulates the impact of AI on elections, in order to guarantee the protection of democratic rights and guide the search for mimetic technological neutrality, based on the promotion of security, transparency, auditability and “explainability” and non-discrimination, among other values in question.

The following lines present some of the regulatory initiatives adopted around the world.

1.1. Brazil

Brazil is holding one of the largest technological elections in the world, with more than 155 million voters and a number of electronic ballot boxes amounting to more than 500,000 units. The country's Superior Electoral Tribunal (TSE by its Portuguese acronym)

has been a pioneer in the use of electronic voting systems since 1996. However, in a context of growing political polarization and intense contamination of the information ecosystem (Rubio Núñez; Monteiro, 2023), Brazil has faced significant challenges in maintaining social trust in the electoral justice system, in voting machines, and in the elections themselves. In this context, the possibilities derived from the use of artificial intelligence systems in electoral processes force the country to prepare for new challenges.

In Brazil, there is still no formal legislation specific to the use of artificial intelligence in general. However, regulatory initiatives are being discussed in Parliament, such as Bill 21/2020, which aims to “allow the development and application of safe and reliable AI, in line with the values and principles of the Federal Constitution.” In general, the bill is based on three fundamental pillars: a) guaranteeing a set of rights to people directly affected by AI systems; b) categorizing the levels of risk associated with these systems and the algorithms based on this technology; and c) implementing governance measures for companies and organizations that provide or operate such systems (Rubio Núñez; Alvim; Monteiro, 2024).

The lack of a specific regulatory framework on artificial intelligence (AI) and disinformation, coupled with the imminent risk that the inappropriate use of these resources represents for electoral processes, has placed the Superior Electoral Tribunal (TSE), in charge of organizing elections and judging conflicts arising from them, as the protagonist in the adoption of regulatory measures. Making use of the prerogative provided for in Article 57-J of the Electoral Law (Law 9,504/97), the Superior Tribunal approved an unprecedented set of provisions to regulate the use of intelligent systems in campaigns. Through Resolution 23,732/2024, the regulation of electoral propaganda, Resolution 23,610/2019, was profoundly modified with the inclusion of Articles 9-B to 9-H, which specifically deal with the use of AI in Brazilian elections.

The new resolution expressly allows the use of generative artificial intelligence in the production of content, as well as authorizing the use of synthetic intelligence solutions to improve, modify or adapt communication materials (art. 9-B). The rule explicitly allows the use of IAGen in the complete creation of content, the modification of aesthetic, sound or textual elements, the elimination of vocal or visual components, the combination of audio and images, the adjustment of playback speed, the superposition of recordings (for example, integrating a studio recording with an external one) or sounds (such as prioritizing the voice of one speaker over another simultaneously).

In order to improve transparency in the use of AI in elections, it was required, as a general rule, that any synthetic content, whether partial or total, be accompanied by an explicit warning—"prominent and accessible"—in order to ensure that the public is not

misled about the origin or nature of the material presented. In this regard, the ETC's regulations, in the use of its regulatory power, follow the guidelines set out in a report by the European Commission, which underlines the importance of transparency in mitigating the risk of manipulation (Denemark, 2024).

The regulation establishes how the warning about the use of AI must be made (§1), as follows: a) at the beginning of pieces or communications made by audio; b) by labelling (watermark) and in the audio description, in pieces consisting of static images; c) in the manner provided for in points a and b, in pieces or communications made by video or audio and video; d) on each page or side of the printed material in which content produced by artificial intelligence is used. The resolution foresees some situations in which the duty to warn is exempt, such as in the case of a) alterations that only serve to promote better image and sound quality, b) the inclusion of visual identity elements, cartoons or logos, and c) the usual image editing resources that promote montages in which the candidate appears alongside supporters. The logic behind this provision rests on the idea that these situations do not have the power to deceive the voter, so as not to be configured as a "cognitive determinant of the vote" (Rubio Núñez; Alvim; Monteiro, 2024). Therefore, excesses in the use of these resources, such as the use of de-aging (artificial rejuvenation) and makeover (deep visual change) techniques, make the warning about the use of AI mandatory, according to Brazilian regulations.

Another important provision concerns the express authorization for the use of chatbots and avatars in campaigns, which also requires the submission of a disclaimer on the use of the resource (§3). To avoid doubts and deception, the regulations prohibit the simulation of dialogue with any human being, whether candidate or not. Failure to comply with this provision imposes the immediate withdrawal of the content and unavailability of the service, either at the initiative of the application provider or by court order (§4).

Regarding the use of synthetically produced or manipulated content to generate disinformation, the resolution expressly prohibits its use in any type of electoral propaganda with the potential to impact the equality of the contest, causing damage to the balance of the elections or the integrity of the electoral process (9-C). When referring to the preservation of electoral integrity, the rule extends the prohibition of the use of AI to produce disinformation not only to candidates but also against electoral institutions and the authorities that comprise them.

Another relevant aspect concerns the treatment of digital platforms. Given the inadequacy of the self-regulation measures adopted by large technology companies to contain the pandemic spread of disinformation content in previous elections, and the recent

experience of serious anti-democratic attacks in the country (culminating in the failed coup attempt on 8 January 2023), the resolution now requires technology companies to adopt more concrete measures related to the duty of care and the social function of platforms.

In this regard, it established the obligation of providers to adopt and publish measures to "prevent or reduce the circulation of facts that are clearly false or seriously decontextualized" that have the potential to affect the regular process of the election (9-D). It also prohibited application providers from profiting from the dissemination of disinformation that affects the electoral process, prohibiting the commercialization of any form of promotion, including prioritizing search results for the dissemination of content of this nature (§1, 9-D).

In addition, platforms were required, independently of a court decision, to take the necessary measures to put an end to the promotion, monetization, and access to publications containing disinformation against the integrity of the electoral process. What can be seen here is the construction of standards aimed at promoting proactive and transparent behavior on the part of the platforms, aimed at mitigating the harmful effects of digital disinformation on the democratic environment and electoral contests.

Although some points may be questioned, such as the excessively generic nature of some of the obligations imposed, the regulatory solution responds to a great need, triggering a sanctioning mechanism capable of demanding responsible behavior from digital platforms, through the establishment of a duty of care, the non-compliance of which would mean a "relevant legal omission" (Rubio Núñez; Alvim; Monteiro, 2024) in the application of the electoral law.

In this context, the resolution stipulates, in an open list, some examples of desirable and expected behavior on social media platforms:

- Drafting terms of use and content policies compatible with the established objective.
- Implementation of effective reporting tools and accessible information channels for both users and public and private institutions.
- Planning and execution of corrective and preventive actions, improving content recommendation systems.
- Transparency of the results obtained from planning and execution actions, especially in relation to corrective and preventive actions.
- Assessing the impact of their services on the integrity of the electoral process, focusing on the implementation of effective measures to mitigate risks, including gender-based political violence.
- Improve technological and operational capabilities, giving priority to tools that contribute to reducing disinformation (Art. 9d).

When dealing with issues more sensitive to democratic health, the Brazilian resolution transferred the logic of asymmetric regulation based on the magnitude of the risks to electoral discipline (Bioni; Garrote; Guedes, 2023), very common in regulations on the use of AI around the world (Rubio Núñez; Alvim; Monteiro, 2024).

On this point, the Brazilian framework (Art. 9-E) was even more incisive in establishing the joint liability of digital platforms, in the civil and administrative spheres, when they do not promote, during the electoral period, the summary elimination of content and accounts that represent a risk: I) of conduct, information and actions that may characterize crimes that particularly impact the democratic environment, such as the violent abolition of the Democratic Rule of Law, coup d'état, interruption of the electoral process, political violence, among others; II) of the disclosure or sharing of notoriously false or seriously decontextualized facts that affect the integrity of the electoral process, including the voting, scrutiny and vote counting processes; III) serious threats, violence or incitement to physical violence against members and staff of the Electoral Justice and the Electoral Public Prosecutor's Office or against the physical infrastructure of the Judiciary in order to restrict or prevent the exercise of constitutional powers or the violent abolition of the Democratic Rule of Law; IV) hate speech or behavior, including the promotion of racism, homophobia, Nazi, fascist or hate ideologies against a person or group due to prejudices of origin, race, sex, color, age, religion and any other form of discrimination; V) the dissemination of synthetically manufactured or manipulated content, including by AI, in disagreement with the labelling standards established in the resolution.

Despite the good intentions shown in trying to strengthen the liability regime of platforms for the content produced in their digital environment, the truth is that, as presented, the rule assigns to individuals the task of carrying out a scrutiny that is "extremely technical and undeniably typical of the functions of the State-judge", in addition to seeming to clash with the general provision on liability provided for in Law No. 12,965/2014, which establishes the Framework for Civil Rights on the Internet (Rubio Núñez; Alvim; Monteiro, 2024), according to which platforms are only responsible for third-party content in the event of a refusal to comply with specific court orders, within the specified period and following their technical capabilities.

It is also worth noting that the changes introduced in Resolution 23.610 also served to strengthen the legal framework for data protection in Brazil. This is especially relevant given that the issue of data processing in electoral contexts has not been regulated by either the Brazilian General Data Protection Law or the electoral legislation (Rubio Núñez; Alvim;

Monteiro, 2024). On the subject, §4 of Art. 10 establishes that data processing must comply with the purpose for which the data was collected and that the principles and standards of the General Data Protection Law (LGPD) must be observed. It also stipulates that electoral agents must provide clear information on the processing of personal data and create channels for voters to request deletion or removal (art. 10, § 5). Also along these lines, §9 of Art. 28 stipulates that the LGPD standards must be observed for electoral advertising that involves the processing of sensitive personal data.

Although it is still too early to draw definitive conclusions about the practical results of the Brazilian regulations on the use of AI, it is possible to identify that the regulatory architecture adopted reflects the brief (but profound) experience that the country's electoral system has had in combating disinformation in digital campaigns and the innovative, agile and successful solutions it has devised to guarantee the integrity of its electoral process.

1.2. *United States*

In the United States, AI has been used frequently in disinformation campaigns during the presidential election, including robocalls imitating President Biden’s voice and fabricated photos of former President Donald Trump being arrested. Cases like these raise questions about the limits of these tools in electoral contexts and are an important part of the debate on AI in elections.

By the end of July 2024, 151 bills on deepfakes and misleading media in the electoral context had been registered on US soil (Norden; Narang; Protzmann, 2024). This figure represents about a quarter of all bills introduced on the general topic of artificial intelligence in the country. In general, these regulations aim to regulate disinformation against candidates or behavior that unduly influences voters.

In recent years, several state laws have been passed on the use of deepfakes. While some of these laws prohibit the use of deepfake resources and other deceptive means in electoral campaigns, others allow their use, requiring certain conditions for their use, such as labeling indicating their use, to offer transparency to the electorate. The variation in approaches to the issue reflects the ideological diversity of states such as California, Minnesota, Texas, Washington and Florida (Rubio Núñez; Alvim; Monteiro, 2024).

Regulations dealing with far-fetched falsehoods and other misleading media in elections also vary in the period of ban or limitation, with some setting a pre-election deadline

for banning (typically 60/120 days) and others making restrictions permanent (Norden; Narang; Protzmann, 2024).

In Minnesota and Texas, the use of deepfakes to influence elections is considered a criminal offense when they are produced or disseminated in the 90 and 30 days prior to the election, respectively, with penalties varying depending on the severity of the act. Washington has more comprehensive regulations that make it easier for victims to access injunctive relief or other forms of redress. The regulations require labeling of manipulated content and allow harmed candidates to sue those responsible for communications with "deepfake" content, although media outlets are exempt from liability in some situations. Finally, Florida imposes an obligation to label any AI-generated material that creates a false appearance of reality to attack a candidate or influence electoral issues. Failure to comply with these regulations can lead to criminal penalties (Rubio Núñez; Alvim; Monteiro, 2024). Another example of a regulatory initiative comes from Mississippi, which passed legislation providing for criminal penalties for distributing digital content without consent in the 90 days before an election, to harm a candidate, prevent the exercise of the vote or influence the election.

As we have seen, the manipulation of information in electoral contexts has not only served to generate advantages for candidates but also as a method to fuel the discredit of electoral institutions and encourage the illegitimate challenge of results. In this regard, strengthening trust and protecting electoral officials from intimidation, harassment, and threats is essential for the normal and peaceful development of elections. The use of AI resources for the widespread and selective production and dissemination of misleading synthetic content poses a real challenge here.

In early October 2024, a series of bills were introduced to the Governor of California. Although the initiative most anticipated by advocates for more comprehensive regulation was vetoed—SB 1047, which stipulated that companies would have to test their AI systems before launching them—bills were signed that increase transparency and accountability in the use of artificial intelligence in elections (Lima-Strong, 2024). The approved texts oblige digital platforms to remove or label misleading or digitally manipulated material about elections (AB 2655), to provide transparency on content used in elections that has been produced by AI (AB 2355). In addition, a law was passed that increased the deadline for prohibiting the distribution of materially misleading content about candidates for a period of 60 days before elections to 120 days after (AB 2839).

Regarding the protection of the electoral process itself, the state of Kentucky debated a bill—which was not approved—to penalize the dissemination of deepfakes that

could affect the development of administrative processes, including, in this case, the administration and results of an election (KY House Bill No. 45). The states of New Jersey (NJ House Bill No. 736) and Illinois (IL House Bill No. 4763) continue to debate bills to regulate the use of deepfakes that affect electoral processes (Norden; Narang; Protzmann, 2024).

The regulation of the use of chatbots in electoral contexts has also been the subject of debate at both the state and federal levels. Several states have considered requirements for the use of this functionality, such as the need for prior identification that the user is interacting with an artificial intelligence system (NY Assembly Bill No. 9103), the display of a warning that the system may be inaccurate or inappropriate (NY Assembly Bill No. 10103) and also the requirement of affirmative consent by the user (CA Assembly Bill No. 3211). These transparency and prior consent requirements have also been required in bills that discuss—as yet undefined—the use of synthetic voice in automated calls in the context of electoral disputes (Norden; Narang; Protzmann, 2024).

Some states are also exploring the possibilities of AI systems helping to solve long-standing challenges in their electoral systems, such as the problem of redistricting, and protecting the distribution of the electorate from gerrymandering. Others are advancing projects that, although not directly related to the electoral process, can produce indirect effects on American elections, such as proposals requiring the inclusion of watermarks on AI-generated content (AB-3211 California Digital Content Provenance Standards; OK House Bill No. 3453), as well as the creation of sanctions against deepfakes for "illegal use" and measures related to the protection of user privacy (Norden; Narang; Protzmann, 2024).

In addition to the regulatory treatment developed by the states, the Executive Order on the Safe and Trusted Development and Use of Artificial Intelligence (White House, 2023) was published at the end of 2023, which regulates the exploitation of the potential applications of AI systems and the management of the risks that accompany these innovative actions. Created to balance the positive and negative aspects of AI against the challenges that have arisen with the rapid advancement of the functionalities of AI systems, the Order offers elements that serve as a parameter to guide the understanding of what can be understood as the safe and reliable use of AI applications undertaken by the Public Administration, even serving as a reference for international regulatory action (Barbosa, 2023). This document presents objective guidelines for the action of government entities, in particular about: a) standards and standards relating to security in applications that use AI systems (Section 4); b) promotion of innovation and competitiveness among actors (Section

5); c) respect for rights, including those of workers (Section 6), civil rights (Section 7), consumers and others (Section 8); d) protection of privacy (Section 9).

Although the vast majority of debates are still under construction, and a considerable number of initiatives are still legislative projects, the evolution of discussions in the United States, while indicating a change of attitude toward the challenges posed by the use of AI in electoral contexts, also suggests the advent of a new regulatory environment for future elections.

1.3. *Canada*

In Canada, automated decision-making has been regulated since 2019 to reduce the risks of error and discrimination. This approach ensures a prominent position for transparency requirements, including the obligation to inform that the decision will come from an automated system, the duty to make public any source code used by the Public Administration, as well as the adoption of precautionary measures aimed at the prior detection of unintentional biases in the data, the monitoring of the results of these decisions and the guarantee of human intervention and the appealability of decisions (Rubio Núñez; Alvim; Monteiro, 2024).

In the electoral dimension, a bill (C-65) was introduced in March 2024 proposing amendments to the Canada Elections Act—already updated by the Elections Modernization Act (2018)—to increase trust and participation in the electoral process. This broad-based bill includes proposals aimed at protecting the integrity of the electoral system from technological threats, such as the misuse of artificial intelligence (AI) and deepfakes (Government of Canada, 2024). AI, in particular, is mentioned in the text in a context of concern about the spread of disinformation and the risk of manipulation of the electoral process.

1.4. *Europe*

At the European level, initiatives have been identified both within the EU and within individual countries.

European Union

In the European Union, the European Council approved the Artificial Intelligence Law (AI Act) in May 2024, based on the recommendations of a High-Level Expert Group on Artificial Intelligence (AI HLEG) created by the European Commission. It aims to regulate the development, use, and impact of AI in various sectors, creating a solid and balanced regulatory framework that promotes technological innovation while protecting fundamental rights.

The regulations are structured from a risk-based approach, classifying AI systems into four categories:

1. **Unacceptable risk AI:** These are systems that are considered a threat to the security, human rights, and fundamental values of the European Union. AI systems that use cognitive manipulation, subliminal or deceptive techniques, social scoring, exploitation of vulnerabilities such as age or economic status, and mass surveillance, among others, are considered prohibited.
2. **High-risk AI:** These are systems applied in sensitive sectors such as healthcare, critical infrastructure, education, and, in particular, democratic and electoral processes. These systems are subject to strict compliance requirements, including audits, transparency, data security, and human oversight.
3. **Limited-risk AI:** AI that has few implications for fundamental rights and does not require major restrictions, being subject to more lax transparency obligations to help users make informed decisions. Examples include simple chatbots or recommendation systems.
4. **Low-risk AI:** These are systems that do not pose significant risks and can therefore operate without regulation. Most AI systems in operation fall into this category.

Despite its general nature, the document contains some provisions that directly influence electoral processes, such as the specific transparency obligations imposed on systems that interact with individuals or that manage content that poses a risk of identity theft or deception, currently commonly used in electoral campaigns to facilitate interaction between candidates and voters.

Furthermore, the AI Law prohibits AI systems capable of promoting manipulative, subliminal or deceptive cognitive influences on the formation of voters' will, as these tools entail unacceptable risks under the prism of individual freedoms and the defense of democracy. With this measure, the law prevents the exploitation of vulnerabilities of certain

social groups, thus prohibiting IT solutions that promote mass surveillance as a way of obtaining data that trigger voter micro-segmentation.

The law also regulates the use of high-risk systems that may threaten essential infrastructures related to the electoral process, such as the regular functioning of electoral bodies, political parties, and institutions in charge of managing the electoral census or issuing the documents necessary to vote, among others. All AI systems in this category must guarantee: a) a robust data governance model, maintaining quality standards and eliminating bias and discrimination; b) security and human supervision in all cycles; c) transparency regarding their operation; d) registration in a community database; and e) passing a compliance test, with the corresponding certification (Rubio Núñez; Alvim; Monteiro, 2024).

Even in relation to systems that offer a medium or low risk, which do not present a significant danger—such as basic chatbots—the regulations also apply, requiring minimum transparency measures that allow users to understand their operation and their main attributes (Rubio Núñez; Alvim; Monteiro, 2024).

Germany

Germany has developed a comprehensive legal framework covering the regulation of artificial intelligence and digital technologies. The logic of this regulatory system is based on a strict legal regime of personal data protection, transparency, and accountability. This regulatory system increases the possibility that AI systems will be used in a way that preserves democratic values and electoral integrity.

The central regulatory basis is the General Data Protection Regulation (GDPR), implemented in 2018. This regulation is one of the most comprehensive pieces of data protection legislation in the world, setting strict privacy standards for all members of the European Union. The GDPR profoundly influences the way political parties and candidates collect, manage and use personal data, especially for electoral targeting, with important implications for the application of technologies such as AI in electoral campaigns (Sapada; Arif, 2024). There are rights to know for what purposes their data is being used, to have access to their data and to have that data rendered useless. Under this legislation, explicit user consent is required for organizations to process private data (Article 6).

At the same time, the German Social Media Enforcement Improvement Act (NetzDG), passed a year earlier, imposes on digital platforms the obligation to remove illegal content within 24 hours of being notified by the users concerned. It also requires technology

companies to produce semi-annual transparency reports and establishes a subjective liability regime, whereby providers become liable when they are found to have systematically and repeatedly failed to comply with the new legal requirements, especially when dealing with user complaints about illegal content. In short, NetzDG aims to restore the health of the information environment by designing a model based on the "obligation to remove content through indirect supervisory liability (Störerhaftung)". (Eifert, op. cit., p. 164).

United Kingdom

In March 2023, the UK Government published a document entitled “A pro-innovation approach to AI regulation”, also known as the “UK White Paper”. This policy document laid out proposals for implementing an innovation-friendly regulatory framework for the use of AI systems in the UK (UK Government, 2023).

Five cross-cutting principles were envisaged to guide and inform the development and use of systems across all sectors, thereby providing the basis for defining the UK’s regulatory approach: a) safety, security, and robustness; b) appropriate transparency and explainability; c) fairness; d) accountability and governance; and e) challenge and redress.

Following the end of the consultation period, the Government published a response to the comments received, responding to criticism that it was difficult to extract from this regulatory framework adequate protection against systemic risks such as disinformation and interference in elections.

The document recognizes the need to protect democracy from AI-mediated electoral interference, and a specific section on the topic has been included, entitled “Protecting democracy from electoral interference”. One of the central points is the strengthening of the Working Group for the Defense of Democracy, which aims to involve experts from various areas of government to mitigate threats, especially foreign interference in electoral processes. This working group demonstrates the intention of the United Kingdom to develop robust prevention strategies, focused on cooperation between different agencies and the use of technical expertise to face the new challenges posed by generative AI.

Another key element of the UK’s regulatory approach is the review of existing electoral laws, which has led to the introduction of a new “digital footprint” regime in the Electoral Act 2022. This measure requires digital campaign materials directed at voters to include clear information about those responsible for creating and distributing this content, such as their names and addresses. The introduction of this obligation increases transparency and allows voters to easily identify the authors of political materials, including

those generated by AI. This way, the Government aims to make it more difficult for AI tools to be used to spread disinformation during the electoral period, promoting greater accountability on the part of those involved in the production of electoral content.

Finally, the British government has proposed watermarking election-related content as a further transparency strategy. This measure aims to ensure that voters have greater confidence in the content they access online, allowing them to better identify authentic material. Together, these strategies reflect a coordinated effort to preserve electoral integrity in the face of the increasing use of AI, preventing manipulation and undue influence on the democratic process (Soon; Quek, 2024).

Ireland

In the run-up to the European Parliament elections in April 2024, the Independent Electoral Commission of Ireland published a Framework on online electoral information, political advertising, and misleading AI content. The document is non-binding, but voluntary, and serves as an indicative guide to good practice in this area. Taking a risk-based approach, the statute addresses both online platforms and search engines, registered political parties, and candidates. The need to ensure a reasonable balance between the exercise of the fundamental rights of freedom of expression and opinion, and participation in public affairs, with the protection of the democratic environment and the integrity of elections has been taken into account when drafting the regulations.

According to the terms of the statute, online political advertising must be used with attention to the principles of transparency and respect for electoral integrity, and must clearly, visibly, and effectively indicate that it concerns electoral content. It is also necessary that relevant actors in the electoral process act to protect elections from disinformation in the digital environment, specifically providing for the creation of an incident reporting mechanism. With regard specifically to the misuse of artificial intelligence systems in electoral processes, the statute states that relevant actors in the electoral process must promote tools to mitigate the risks related to the production of misleading content, including deepfakes. In addition, mechanisms need to be developed to properly label synthetically produced images, audio and videos that may be confusing or misleading (Coimisiún Toghcháin, 2024).

1.5. *Other Experiences*

India

In India, political parties have spent over $50 million on AI-produced content by 2024, including deepfakes of deceased political figures (Dutt, 2024) and image manipulation of celebrities. Although the Election Commission of India (ECI) has an IT-oriented regulatory framework (the IT Act) that generally regulates internet platforms, it has found it difficult to address the irregular use of social media and messaging services in elections, especially since the code of conduct governing behavior on social platforms is not binding (Gupta; Mathews, 2024).

In the face of repeated instances of irregularities, the ECI sent a communication to all political parties calling for ethical and responsible use of social media platforms and highlighting, among several regulatory provisions, Section 66D of the Information Technology Act, which provides for punishment of persons who use communication or computing devices with malicious intent, such as misleading identity or deception (Indian Express, 2024). However, in the absence of more effective legal mechanisms, the consequences of violations are usually not severe (Gupta; Mathews, 2024).

India currently lacks a specific regulatory framework for AI. However, given the growing number of cases involving the misuse of intelligent solutions in electoral processes, including an episode where the Gemini tool (developed by Google) submitted a response suggesting that some experts understood the Indian Prime Minister to have pursued fascist policies (Dhillon, 2024), demands for regulation have been increasing (Gupta; Mathews, 2024). In July, it was reported that the Ministry of Electronics and Information Technology is drafting legislation focused on AI, which will require labeling of AI-produced content. It is also studying legal parameters for large language models (LLMs) to be trained in Indian languages and with content specific to the local context (Barlk, 2024).

South Korea

In South Korea, an amendment to the Public Official Election Act came into effect in January 2024, banning the use of AI-produced deepfakes in the 90 days before election day. As a result, Section 82(8) of the law now states that: “[n]o one may produce, edit, distribute, display, or publish deepfake videos for election campaign purposes from 90 days before

election day until election day" (National Election Commission of the Republic of Korea, 2024). The law provides for a penalty of up to seven years in prison or a fine of around $35,000 (Soon; Quek, 2024). Furthermore, the use of clever tools to promote political participation through the production of campaign slogans, jingles, and speeches is permitted in Korean elections (Chakravarti, 2024).

Singapore

Singapore's approach to using AI in elections is characterized by a focus on transparency, accountability, and mitigating threats of disinformation and foreign interference. Although the country does not yet have regulations targeting AI in elections exclusively, Singapore has adopted a regulatory framework that covers three main areas: disinformation, political propaganda, and foreign interference (Soon; Quek, 2024). Documents such as the Protection from Online Falsehoods and Manipulation Act (POFMA) and the Foreign Interference Countermeasures Act (FICA) aim to combat the spread of false information and external influences that may jeopardize the integrity of elections.

Furthermore, Singapore enforces strict transparency requirements in political advertising, especially in the online context. The Parliamentary Elections Act and the Presidential Elections Act set disclosure requirements for election advertisements, including identifying who is funding and authorizing the content. These measures help ensure that the public can verify the source of information, minimizing the impact of disinformation or manipulation campaigns, potentially reinforced with the use of AI (Soon; Quek, 2024).

In September 2024, the Ministry of Digital Development and Information (MDDI) introduced a draft Election Bill seeking to include new, more effective safeguards against digital manipulation of content in electoral processes, including the use of artificial intelligence systems to produce deepfakes. The bill proposes to ban the publication of digitally generated or manipulated electoral advertising content that realistically shows a candidate saying or doing something that did not happen. It also provides for the possibility of issuing corrective instructions for the removal of offensive content or disabling users' access to such content in the country, with penalties of fines, imprisonment, or both for failure to comply with these measures (Government of Singapore, 2024). Candidates who publish false or misleading content are exposed to fines or even the loss of their seats (Iau, 2024).

6. Jurisdictional Approach

Judicial decisions on the use of AI in elections are still rare in electoral tribunals, either due to the absence or the youth of specific laws, depending on the case. Therefore, there remains great uncertainty about how to interpret the few legal provisions that are gradually appearing.

In August 2024, the Specialized Chamber of the Electoral Tribunal of the Federal Judiciary of Mexico analyzed an advertisement based on the image of a child synthetically created by a political party in an electoral context. In its first meeting with the subject, the Court ruled that the use of this type of image could endanger the best interests of the child, contrary to the Mexican Constitution. According to the ruling, this form of propaganda characterizes the instrumentalization of childhood for political purposes, which implies a violation of the rights of children and adolescents. The use of children's images in electoral processes, therefore, must be accompanied by a higher logic of care and protection. The Specialized Chamber of the Court concluded that the use of the image of a minor through the use of AI technology by an electoral campaign exceeds the limits of the use of propaganda since it is a simulation that seeks to circumvent national legislation (SRE-PSC-369/2024). However, the Superior Chamber of the TEPJF revoked, by majority vote, the aforementioned ruling, considering that the image itself does not expose the rights of children to potential danger. In SUP-REC-893/2024 it was decided that the circumstances of each case must be considered and that the use of the representation created with AI does not correspond to the use of the image of a minor.

When analyzing electoral propaganda using deepfakes, within the framework of the recent regulation of the Brazilian TSE (Resolution 23,610, updated in 2024), the Regional Electoral Court of São Paulo, in Brazil, held that to characterize an irregularity, the creation or manipulation of content with synthetic resources is not enough, but it is necessary to verify whether the use of these instruments produced propaganda with plausibility and effective potential for harm (REl 060005354). The case concerned a video in which the face of a candidate for mayor of São Paulo was presented in an ultra-realistic way, replacing that of the character "Ken" from the movie "Barbie." The Court ruled that the content was legal, given the low quality of the editing. It thus established the perception that illegality depends on the "minimal possibility" of convincing the voter.

In turn, the Regional Electoral Court of Minas Gerais, also in Brazil, imposed a fine on a candidate who used in his campaign the image of his late grandfather, who had been mayor for four different terms. For the Court, the mere indication of the nature of the synthetic

content did not exclude the illegality of the advertisement, given the express violation of electoral legislation (REI 060080847). In another decision, the Court held that the dissemination of digitally manipulated content with the intention of defaming candidates constitutes irregular negative advertising and justifies the granting of a court order to provide data identifying those responsible, to protect the integrity of the electoral process (REI 060061190).

In the United States, in October 2024, part of a new law enacted by the State of California less than a month ago, allowing anyone to sue for damages arising from election deepfakes, was suspended by a federal judge. According to the judge, the law appears to violate the First Amendment of the Constitution, as it "unconstitutionally stifles the free and unfettered exchange of ideas" (Healey, 2024).

7. Classification of Results

Taking into account the methodology outlined in Chapter 2 of this report, the regulatory standards found are now classified from ten different perspectives.

In terms of **breadth**, we find regulations that give AI a systematic approach, such as the European Union's AI Law, which, while not dealing with electoral matters in a restricted manner, has effects on the dynamics of the organization of elections. On the other hand, cases were also identified in which intelligent computing receives (or tends to receive) comprehensive treatment within the electoral system, this being the direction adopted by Resolution 23.732/2024 of the TSE of Brazil, as well as the draft reform to the Electoral Law of Canada, emblematic cases of a micro-systematic approach. Specific treatment, however, appeared more frequently within the sample, especially in concise and specific laws approved, for example, in California (AB 2355, AB 2655, and AB 2839), which imposed specific obligations on digital platforms about the misuse of AI systems in electoral contexts, in addition to extending the period in which the dissemination of misleading material is prohibited. Similarly, specific modifications were found in South Korea, in a provision prohibiting electoral exploitation of deepfakes.

Regarding the **scope of legal intervention**, no constitutional amendments have been identified that regulate the issue, which can be explained both by the fact that electoral regulations, as a rule, reside in infra-constitutional norms and by the fact that, also as a general rule, constitutional amendments imply a much stricter procedure for their approval. However, there have been important regulatory developments at the EU level, with the

European AI Law, and also at the legal level, with the enactment of standards that raise the level of protection offered against the risks of AI systems, such as the various US state laws regulating the use of deepfakes in elections. There has also been at least one regulatory initiative directly derived from an Electoral Justice body: the Brazilian model, in which resolutions, although secondary normative actions have the same status as formal laws.

In terms of the **premise of the regulatory matrix**, there were both risk-based approaches, such as the AI Act and the German General Data Protection Regulation (GDPR), and hybrid ones, such as the Brazilian bill to regulate the use of AI, which focuses on both preserving rights and understanding the risks posed by AI systems, more rigorously calibrating models that carry higher risks.

In terms of the **scope of the regulations analyzed,** those that establish a duty of care imposed on platforms and the liability of political actors predominate, as can be seen in the case of the Indian law on information technologies and the South Korean legislation, which establishes punishments in the event of the production and dissemination of malicious content (in the latter case, with the possibility of prison sentences). We also find data protection regulations that have a considerable impact on electoral processes, such as the general data protection laws of Germany and Brazil. We also find regulations that hold platforms responsible for non-compliance with court orders, such as Resolution 23.610 of Brazil and the recent draft law of Singapore.

Analyzing the **recipients of the sanctioning standards**, we observe that most of the regulations are directed at candidates' partisan entities content producers, and politicized people in general (i.e. those responsible for producing/manipulating and disseminating irregular content using AI resources), as in the case of the Irish statute and the Brazilian Resolution. We also identify regulations directed at producers, developers, and providers of artificial intelligence systems, especially risk-based regulations such as the AI Law.

As for the **nature of the sanctions** envisaged, some regulatory experiences include the removal of content, such as the Singapore Bill, the NetzDG, and the Brazilian Resolution. Financial fines were also identified in the German GDPR and NetzDG, the AI Act, and the Brazilian Resolution, as well as the possibility of prison sentences in provisions of South Korean legislation and the Singapore Bill. There are also legal norms in which the consequence of the misuse of AI in elections is punishable by the loss of mandate (Singapore Bill)—and, in addition, by the ineligibility of the person involved (Brazilian Resolution). It should be noted that Brazilian legislation also provides for the suspension of Internet application services in the event of non-compliance, as well as the banning or

suspension of profiles and groups or social media channels dedicated to disinformation. From there came the temporary suspension of the operation of the X platform in the country, as a last resort measure following the systematic refusal to comply with orders to block accounts of important actors spreading disinformation against electoral integrity.

In terms of the **levels of legislative action**, the Brazilian Resolution lists a series of measures aimed at platforms, to stop the dissemination of irregular synthetic content in electoral processes. Various obligations have been established, including the need to be authorized to provide political-electoral services, as well as measures that affect the business model (such as developing and applying conditions of use and content policies compatible with the objectives of the resolution, implementing complaint and notification channels, transparency of results, etc.). It should be noted that these requirements have led some platforms, such as Google, to announce that they will not allow the dissemination of paid political-electoral content (Agência Brasil, 2024).

Along similar lines, in Europe, the AI Law established various mandatory measures for the operation of intelligent systems, with higher levels of rigor for those that offer greater systemic risks, including obligations of prudence about algorithmic programming. Controlling inappropriate behavior was a predominant focus in the documents studied, with prohibitions on the use of bot agents and fake user profiles, as well as restrictions on the use of mass activation tools in Brazil. We also found a recurrence of a rigid stance on content control, with most instruments establishing legality parameters for advertising content. An example of this is seen in the treatment of the issue by the various American States studied, which prohibit false content using deepfake technology.

In regard to the **legal rights protected by content limitation standards**, the measures usually simultaneously protect various legal rights that are desirable in the electoral process, such as freedom of suffrage, equal opportunities, the honor and dignity of candidates and the image and trust in electoral institutions. Although not explicitly stated, the intentions can be understood from standards that point out the harmfulness of misleading content that causes cognitive embarrassment or hinders the conscious exercise of citizenship.

The German General Data Protection Act is one of the regulations that best demonstrates an approach aimed at protecting users' right to privacy. Regarding the protection of vulnerable or minority groups, it was possible to identify restrictions on the use of AI systems based on social scoring, economic conditions, or other analyses of personal characteristics that imply discrimination. A relevant example is the prohibition of AI practices in EU legislation, especially when it prohibits the marketing of services using AI that impose

unfavorable treatment on people or social segments in an unjustified and disproportionate manner (Art. 5, 1, c of the EU AI Law). As a general rule, all the regulations studied are aimed, albeit indirectly, at ensuring the peaceful nature of elections and democratic stability and social peace, although Brazilian regulations that combat violence, incitement to hatred, extremism and radicalization do so more visibly.

In regard to the **degree of coverage of the risks mapped**, we find a predominant focus on the risks arising from electoral disinformation and its impact on human rights, which sometimes results in AI being treated only as part of efforts to combat information disorders in the context of elections. In this regard, for example, the case of South Korea. Concern about the increase in political violence, discrimination and harassment is observed in some regulatory efforts that also cover conflict prevention, such as the Brazilian resolution, which provides for specific treatment in relation to conduct that characterizes actions of political violence and discrimination. Finally, control targeting the irregular use of personal data was widely verified in the regulations studied, as observed in the German and Brazilian general personal data laws, as well as in the legislation of the European Community.

8. Conclusion and Catalogue of Recommendations

The inability to adapt to technological transitions calls into question the ability of electoral administration bodies to respond adequately to the dissemination of harmful content that circulates intensively in digital media. In this sense, the technical training of internal teams can be seen as a prerequisite for the materialization of agile and effective responses that avoid or mitigate the damage associated with crisis scenarios.

It is therefore essential for electoral institutions to establish partnerships with entities specialized in technology and data protection, in order to better understand the tools used to spread harmful narratives and develop appropriate strategies to counter them (Goltzman; Lopes, 2024). After all, the knowledge gap in this specific area "is not merely superficial, but fundamental for the effective application of justice in a technologically saturated context" (Tavares, 2024).

The increasing use of artificial intelligence in electoral processes, especially at the national level, demands a robust, timely and technically appropriate regulatory approach that takes into account both the mitigation of risks and the creation of mechanisms to discourage harmful practices, as well as the maximization of the benefits that this technology potentially offers. Through this lens, electoral bodies should closely follow legislative

movements, with a view to ensuring that, to the extent possible, agendas related to the protection of electoral mechanics are presented.[20]

Furthermore, it is up to the electoral justice bodies to adopt creative and comprehensive strategies to ensure that intelligent computing, within the scope of their powers, is used ethically and in accordance with democratic principles, taking into account the warning that "postponing the confrontation of this issue will increase the level of difficulty in containing and correcting the harmful effects already caused" (Tavares, 2022). Moreover, for the moment it is appropriate to admit, without further ado, that "it is not possible to confront the evils of AI without AI" (Rubio Núñez; Alvim; Monteiro, 2024).

Seeking to systematize and expand a path initially paved by a wide range of authors (Assibong et al, 2019; Chennupati, 2024; Juneja, 2024; Muñoz, 2024; Ogwuche; Onah, 2023; Panditjaratne; Giansiracusa, 2023; Rubio Núñez; Alvim; Monteiro, 2024; Sook; Quek, 2024; Tuset Varela, 2024; Yazbek, 2024; Yu, 2024), we present a list of recommendations for the democratic application of artificial intelligence in campaigns and electoral processes:

1. **Establishing specific standards for the use of AI:** Regulation should provide for a specific framework that addresses the particularities of AI in the context of the contest for votes, focusing on ensuring that its use does not compromise the integrity of the electoral process. Clear standards should be established to prevent the spread of disinformation, the breaking of the authenticity of public dialogues with the participation of bots, and other forms of undue interference. Mandatory disclosure of the use of AI, including the labeling of AI in communication documents, and public disclosure of data mining and voter segmentation resources are crucial steps in this regard.
2. **Transparency and accountability:** A high degree of transparency should be required about the use of AI in campaigns and electoral administration processes. This includes the obligation to make public the use of algorithms for voter segmentation or content generation, as well as the criteria used by these systems. Accountability is essential to ensure that the practices adopted respect voters' rights and the principle of equal access to information.
3. **Expanding regulatory oversight:** Expanding the regulatory scope to explicitly include AI is critical. The current electoral legal regime must be adapted to take into account the impacts of AI in all phases of the electoral process, from campaigning to vote counting, promoting continuous and effective oversight. An important part of these

[20] Despite all the difficulties, it is vital to realize that, given the issues discussed above, regulatory inertia must also be understood as a huge risk in itself (Sapada; Arif, 2024), since the absence of standards, conditions and limits exposes electoral competitions to a new collection of very concrete and significant technological dysfunctions.

efforts is establishing a data regulatory framework capable of safeguarding data subjects, ensuring lawful and fair access, and preventing misuse.

4. **Cooperation with the technology sector:** Interaction with digital platforms and leading AI companies should be expanded. A continuous dialogue between electoral bodies and the private sector will allow for a better understanding of technological challenges and provide input for the creation of regulations that are technically feasible and appropriate to the electoral context. Eventually, these approaches could result in specific agreements to adapt products to social needs. In addition, it is important to require social media providers to adapt their terms and conditions to the context, update them, and apply them in a clear, coherent and impactful manner. Measures to increase registration barriers, eliminate bots, and reduce the alteration of the authenticity of virtual dialogues are essential from this perspective. The same can be said of the insertion of elements of friction to hinder access, sharing, viralization, and involuntary consumption of harmful content.

5. **Civil society participation:** The participation of civil society organizations, technology experts, and political rights groups is essential to legitimize the regulatory process. Creating institutional mechanisms to listen to and consider the concerns and suggestions of these actors can reinforce public confidence in elections and ensure that regulation is sensitive to social demands. It is also important to build an agenda aimed at fostering innovation. Finally, electoral management bodies should seek agreements with strategic actors that can meet part of their strategic needs, to expand their institutional capacities.

6. **Continuous monitoring and evaluation:** The dynamic nature of AI technologies requires a regulatory approach that allows for the periodic review and updating of applicable standards. The creation of advisory committees made up of experts in AI, data science, political communication, and digital law, as well as the development of qualitative research with professionals in these areas, can ensure that regulation remains up to date with technological innovations and new emerging risks.

7. **Identifying beneficial applications of AI:** In addition to regulation aimed at mitigating risks, it is important to identify and encourage the use of AI to improve the security, efficiency, reliability, and accessibility of electoral processes. However, artificial intelligence should be seen as a means to achieve fundamental objectives, and not as an end in itself. In this regard, electoral organizations should think about how to apply artificial intelligence to achieve the objectives contained in their strategic planning, and not how to adapt their strategic planning to somehow accommodate some AI solutions.

8. **Responsibility of platforms and users:** The regulatory standard must guarantee the attribution of responsibility both to the developers of AI technologies and to the candidates and political parties that benefit from their applications. There must be clear provisions to demand responsibility from those who allow or use AI in a way that endangers the legitimacy of the electoral process, through proportionate and effective sanctions, avoiding, as far as possible, the imposition of sanctions based on generic prohibitions, with open clauses that generate legal uncertainty as a consequence of a high degree of abstraction.

9. **Sanctions and sharing of responsibilities:** The adoption of a clear and proportionate sanctions regime is crucial to inhibit the misuse of AI. The regulation should provide not only for sanctions for candidates and parties that misuse intelligent computing, but also for accountability for digital platforms and technology providers that facilitate these practices. Sharing responsibilities among all actors involved will contribute to the effectiveness of the regulation and the protection of the electoral process.[21]

10. **Promote media literacy and information education**: Investing time and energy in educational projects can help develop the public's resilience to misinformation. Media education develops critical thinking skills in relation to content, mitigating the excess of credulity that facilitates the internalization of false narratives. On the other hand, it encourages users to use technological tools safely and responsibly, from the Internet to social networks, including artificial intelligence. Information education, for its part, reinforces the evaluation of the credibility of information, training the audience to correctly assess the relevance of discourses, detecting argumentative fallacies and separating valid sources from invalid ones, as well as statements of fact from mere opinions.

10. **Consider the value of algorithmic education and emotional intelligence education:** Algorithmic education empowers users by providing them with a basic understanding of how artificial intelligence and social media platforms work, emphasizing the social impacts of programming. Similarly, emotional education can contribute to a positive transformation agenda, making voters less susceptible to false narratives and argumentative blackmail by raising awareness of the existence of biases, cognitive dissonance, logical processing failures arising from intuitive thinking, and other weaknesses of the sensory apparatus.

11. **Ensure that the adoption of sensitive technologies is preceded by strategic legitimation campaigns:** Public faith in and acceptance of AI is crucial for its effective use

[21] After all, if it is "[...] clear that AI is used both by candidates and campaigns and—sometimes even more intensely—by voters and in different media formats (image, video and audio), [...] regulatory measures or public policies on the subject must take into account the different audiences" (Data Privacy Brasil; Alafialab, 2024).

by electoral management bodies. Lacking sufficient knowledge about the technology, some people may be distrustful or wary, which tends to heighten the overall mood of suspicion. To trust AI and use it in elections, people must understand its benefits, risks, and limitations (Chennupati, 2024).

12. **Establish internal policies to ensure responsible use of AI:** Electoral bodies should stipulate internal principles and guidelines to ensure the safe and responsible use of intelligent tools. These standards should ensure, among other things, transparency, “explainability” and audit mechanisms, as well as provide for monitoring protocols and guarantee human involvement in all artificial intelligence cycles. Rules for periodic review, adaptability, and error correction are indispensable. The effective adoption of AI solutions, however, must be preceded by internal studies that consider a balance between the risks involved and the potential benefits, while ensuring due attention to proportionality in terms of structure, scale, and volume of operations.

13. Encou**rage candidates and political parties to widely adhere to ethical pacts or codes of conduct:** Although they do not have an imposing weight or overwhelming value, ethical pacts and codes of conduct can yield positive results, as an effect of a public commitment assumed by electoral groups and actors, especially in scenarios of regulatory desert.

14. **Activate strategic alliances for a networked response:** Given the global nature of technology and the rapid export of digital disinformation strategies online, new pathologies of political communication represent a common horizon of challenges for electoral organizations. Dialogue and the exchange of knowledge between organizations from different countries, as well as the formation or promotion of academic research groups, can make a difference, since learning from pioneering experiences can avoid errors, eliminate vulnerabilities and qualify the work of institutions.

9. References

ABRANCHES, S. O TEMPO DOS GOVERNANTES INCIDENTAL. SÃO PAULO: CIA DAS LETRAS, 2020.

AGÊNCIA BRASIL. Google no permitirá anuncios políticos en las elecciones de octubre. Agência Brasil, April 24, 2024. Available at: [https://agenciabrasil.ebc.com.br/justica/noticia/2024-04/google-nao-permitira-anuncios-de-politicos-nas-eleicoes-de-outubro]. Consulted: October 21, 2024.

AKBAR, P.; LOILATU, M.; PRIBADI, U.; SUDIAR, S. Implementation of Artificial Intelligence by the General Elections Comission in Creating a Credible Voter List. ICONPO X, No. 717, 2021, pp. 1-7.

ALMEIDA, P. G. R. de; SANTOS, C. D. do; FARIAS, J. S. Regulación de la Inteligencia Artificial: un marco para la gobernanza. Ethics and Information Technology, April, 2021, pp. 505-525.

ALVIM, F. F. ABUSO DE PODER NAS COMPETIÇÕES ELEITORAIS. 2. ED. BELO HORIZONTE: FÓRUM, 2024.

ARAMBURÚ MONCADA, L. G.; LÓPEZ REDONDO, I.; LÓPEZ HIDALGO, A. La inteligencia artificial en RTVE al servicio de la España vacía. Cobertura informativa con redacción automatizada para las elecciones municipales de 2023. Revista Latina de Comunicación Social, No. 81, 2023, pp. 1-16.

ARNOLD, R. Five principles for using technology to support election access and inclusion. International Foundation For Electoral Systems, October, 2023. Available at: [https://www.ifes.org/learning-series-disability-inclusive-election-technology]. Consulted on: 23.10.2024.

ASSIBONG, P. A.; WOGU, I. A. P.; SHOLARIN, M. A.; MISRA, S.; DAMASEVIČIUS, R.; SHARMA, N. The Politics of Artificial Intelligence Behaviour and Human Rights Violation Issues in the 2016 US Presidential Elections: An Appraisal. En: SHARMA, N.; CHAKRABARTI, A.; BALAS, V. E. (Eds.). Gestión de datos, análisis e innovación. Proceedings of ICDMAI, vol. 2. New York: Springer, 2019, p. 295-310.

BAHRI, P. R.; ASMARA, H. M. G.; HUM, M.; RISNAIN, M. Artificial Intelligence (AI)-based campaign in the implementation of general elections. International Journal of Multidisciplinary Research Review, 9 (2), 2024, pp. 117-127.

BALAGUER CALLEJÓN, F. La constitución del algoritmo. Río de Janeiro: Forense, 2023.

BARBOSA, L. P. La nueva orden ejecutiva de EE. UU. sobre Inteligencia Artificial segura y fiable. Jota. Available at: [https://www.jota.info/opiniao-e-analise/colunas/regulando-a-inovacao/a-nova-ordem-executiva-dos-eua-sobre-inteligencia-artificial-segura-e-confiavel]. Consulted: 13.9.2024.

BARCELLOS, A. P. de; TERRA, F. M. La libertad de expresión y los retos de la democracia digital. En: BRANCO, P. G. G.; FONSECA, R. S.; BRANCO, P. H. de M. G.; VELLOSO, J. C. B.; FONSECA, G. C S. Eleições e democracia na era digital. São Paulo: Almedina, 2022, p. 263-286.

BARLK, S. La ley de IA no puede prescribir consecuencias penales para las infracciones. Indian Express. Available at: [https://indianexpress.com/article/business/ai-law-may-not-prescribe-penal-consequences-for-violations-9457780]. Consulted: 17.10.2024.

BARROSO, L.V. B. Libertad de expresión y democracia en la era digital. El impacto de las redes sociales en el mundo contemporáneo. Belo Horizonte: Fórum, 2023.

BENDER, S. M. L. Elecciones algorítmicas. Michigan Law Review, v. 121, Issue 3, p. 489-522 (2022).

BIONI, B.; GARROTE, M.; GUEDES, P. Temas centrales en la regulación de la IA: lo local, lo regional y lo global en la búsqueda de la interoperabilidad regulatoria. São Paulo: Asociación Brasileña de Investigación sobre Privacidad de Datos, 2023.

BOZKURT, B. Policy reccomendations for Electoral Management Bodies. Election Monitor AI, March 1, 2024. Disponível em: [https://electionmonitorai.com/2024/03/01/policy-recommendations-for-electoral-management-bodies/]. Accessed: 23.10.2024.

CARETTI, P; DE SIERVO, U. Diritto Costituzionale e Publico. 3 ed. Turín: G. Giappichelli, 2017.

Carter Center. Carter Center Election Expert Mission to Kenya 2022. Final Report. Available at: [https://www.cartercenter.org/resources/pdfs/news/peace_publications/election_reports/kenya-2022-elections-final-report.pdf]. Consulted: 29.10.2024.

CARRASCÓN, I. Operaciones encubiertas y usos malintencionados de la IA para influir en las elecciones. Newtral, October 7, 2024. Available at: [https://www.newtral.es/ia-influencia-elecciones/20241007/]. Consulted: 08.10.2024.
CHAKRAVARTI, J. AI-Generated Deepfakes Flood South Korean Election Campaigns. Bank Info Security, February 20, 2024. Available at: [https://www.bankinfosecurity.asia/aigenerated-deepfakes-flood-south-korean-election-campaigns-a-24399]. Consulted: 17.10.2024.
CHARAUDEAU, P. La conquista de la opinión pública. São Paulo: Contexto, 2016.
CHENNUPATI, A. K. The threat of artificial intelligence to elections worldwide: a review of the 2024 landscape. World Journal of Advanced Engineering Technology and Sciences, 2024, 12(01), pp. 29-34.
COIMISIÚN TOGHCHÁIN. Framework on Online Process Information, Political Advertising and Deceptive AI Content. Available at: [https://cdn.electoralcommission.ie/app/uploads/2024/04/23163750/Framework-on-Online-Electoral-Process-Information-Political-Advertising-and-Deceptive-AI-content.pdf]. Consulted: 23.10.2024.
CUPAĆ, J.; SCHOPMANS, H.; TUNCER-EBERTÜRK, I. Democratisation in the age of artificial intelligence: introduction to the special issue. Democratisation, v. 31, No. 5, 2024, pp. 899-921.
DEEPAK, P.; SIMOES, S.; MACCARTHAIGH, M. AI and core Electoral processes: mapping the horizons. AI Magazine, v. 44, Issue 3, September 2023, pp. 218-239.
DEGLI-ESPOSTI, S. La ética de la inteligencia artificial. Madrid: CSIC, 2023.
DINAMARCA, J. El riesgo de la inteligencia artificial para la democracia y los primeros esfuerzos de la UE para regularla. The Lawyer Quarterly, vol. 14, No. 1, 2024. Available at: [The Lawyer Quarterly (cas.cz)]. Consulted: 22.03.2024.
DHILLON, A. India confronts Google over Gemini AI tool's 'fascist Modi' responses. The Guardian, February 26, 2024. Available at: [https://www.theguardian.com/world/2024/feb/26/india-confronts-google-over-gemini-ai-tools-fascist-modi-responses]. Consulted: 21.10.2024.
DURAND, T. C. Bulos, choradas e ideas perniciosas. La ciencia detrás de las mentiras que nos cuentan. Barcelona: Plataforma Actual, 2023.
DUTT, B. Los políticos indios llevan a los muertos a la campaña electoral, con ayuda de la IA. Resto del mundo. Available at: [https://restofworld.org/2024/dead-relatives-ai-deepfake-india/]. Consulted: 17.10.2024.
EIFERT, M. The German Social Media Enforcement Improvement Act [NetzDG] and platform regulation. En: ABBOUD, G.; NEY JR., N.; CAMPOS, R. (eds.). Fake News and regulation. 2. ed. São Paulo: RT, 2020, pp. 161-191.
ESTARQUE, M.; ARCHEGAS, J. V. Redes sociales y moderación de contenidos: creando reglas para el debate público desde la esfera privada. Río de Janeiro: ITS-Rio, 2022.
FACHIN, J.; VERONESE, A. Ampliando el debate sobre el Artículo 19 de la Carta de Derechos de Internet de Brasil a partir de una revisión bibliográfica de la Sección 230 del Título 47 del Código de los Estados Unidos. En: FRAZÃO, A; MULHOLLAND, C; POLIDO, F. Bertini P. Marco Civil da Internet. Impactos, evoluciones y perspectivas. 10 anos. São Paulo: Revista dos Tribunais, 2024, pp. 43-63.
FARINHO, D. S. Delimitación del espectro normativo de las redes sociales. En: ABBOUD, G.; NEY JR., N.; CAMPOS, R. (eds.). Fake News y regulación. 2. ed. São Paulo: RT, 2020, pp. 29-90.
FILIMOWICZ, M. Introducción. En: FILIMOWICZ, M. Deep Fakes. Algorithms and Society. Nueva York: Routledge, 2022, p. X-XI.
FISHER, M. La máquina del caos. Cómo las redes sociales han reprogramado nuestras mentes y nuestro mundo. São Paulo: Todavia, 2023.

FREITAS FILHO, R; LIMA, T. M. Metodologia de análise de decisões. Univ. Jus, Brasília, No. 21, jul./dic. 2010, pp. 1-17.

FUX, L.; FONSECA, G. C. S. Moderación de contenidos y redes sociales: un ensayo sobre la libertad de expresión en la era digital. En: BRANCO, P. G. G.; FONSECA, R. S. da; BRANCO, P. H. de M. G.; VELLOSO, J. C. B.; FONSECA, G. C. S. Eleições e democracia na era digital. São Paulo: Almedina, 2022, p. 229-250.

GABRIEL, M. Inteligência artificial: do zero ao metaverso. São Paulo: Atlas, 2022.

GILLESPIE, T. Custodios de Internet. Plataformas, moderación de contenidos y las decisiones ocultas que dan forma a los medios sociales. New Haven y Londres: Yale University Press, 2018.

GOLTZMAN, E. M; LOPES, L. V. de S. Inteligencia artificial, discurso de odio y los límites de la justicia electoral: un estudio sobre la protección de la democracia. Justiça Eleitoral em Debate, v. 14, No. 1, 2024, pp. 65-73.

GOBIERNO DE CANADÁ. El Ministro LeBlanc presenta legislación para reforzar aún más el proceso electoral de Canadá, March 20, 2024. Available at: [https://www.canada.ca/en/democratic-institutions/news/2024/03/minister-leblanc-introduces-legislation-to-further-strengthen-canadas-electoral-process.html]. Consulted: 21.10.2024.

GRIJELMO, A. El arte de manipular a las multitudes. Las técnicas para mentir y controlar las opiniones se han perfeccionado en la era de la posverdad. El País, 28.08.2017. Disponível em: [https://brasil.elpais.com/brasil/2017/08/22/opinion/1503395946_889112.html]. Consulted: 02.09.24.

GUPTA, N.; MATHEWS, N. India's Experiments With AI in the 2024 Elections: The Good, The Bad & The In-between. Tech Policy Pres. Available at: [https://www.techpolicy.press/indias-experiments-with-ai-in-the-2024-elections-the-good-the-bad-the-inbetween/]. Consulted: 17.10.2024.

HAMMAR, Cecilia. Smart Elections: is AI the Next Wave in Electoral Management? IDEA, May 20, 2024. Available at: [https://www.idea.int/news/smart-elections-ai-next-wave-electoral-management]. Consulted: 23.10.2024.

HAN, B. C. Infocracia. Petrópolis: Vozes, 2022.

HARARI, Y. N. Nexus. Breve historia de las redes de información, de la Edad de Piedra a la inteligencia artificial. São Paulo: CIA, 2024.

HAWES, B.; HALL, W.; RYAN, M. ¿Puede utilizarse la inteligencia artificial para socavar las elecciones? Web Science Trust, September, 2023. Available at: [https://eprints.soton.ac.uk/484562/]. Consulted: 30.09.2024.

HEALEY, J. El juez bloquea la ley de California que apuntaba a los anuncios falsos de campaña. Los Angeles Times, October 3, 2024. Available at: [https://www.latimes.com/california/story/2024-10-03/judge-blocks-california-law-that-targeted-deepfake-campaign-ads]. Consulted: October 21, 2024.

HERRERÍAS CASTRO, L. EL CONOCIMIENTO EFECTIVO EN LA JURISPRUDENCIA DEL TRIBUNAL SUPREMO: ¿HACIA UNA OBLIGACIÓN GENERAL DE SUPERVISIÓN? EN: HERNÁNDEZ SAINZ, E.; MATE SATUÉ, L. C.; ALONSO PÉREZ, M. T. LA RESPONSABILIDAD CIVIL POR SERVICIOS DE INTERMEDIACIÓN PRESTADOS POR PLATAFORMAS DIGITALES. A CORUÑA: COLEX, 2023, P. 235-261.

IAU, J. Singapore seeks to fight deepfakes in elections with new laws ahead of 2025 polls. MyNews, September 20, 2024. Available at: [https://www.scmp.com/week-asia/politics/article/3279357/singapore-seeks-fight-deepfakes-elections-new-laws-ahead-2025-polls]. Consulted: 18.10.2024.

INDIAN EXPRESS. Election Commission to parties: don't post deepfakes, misleading info on social media. Indian Express, March 7, 2024. Available at:

[https://indianexpress.com/elections/election-commission-deepfakes-social-media-misinformation-mcc-9312006/]. Consulted: 21.10.2024.
INNERARITY, D. Inteligencia artificial y democracia. París: UNESCO, 2024.
JUNEJA, P. Inteligencia Artificial para la Gestión Electoral. Estocolmo: IDEA Internacional, 2024.
JUNGHERR, A.; RAUCHFLEISCH, A.; WUTTKE, A. Los usos engañosos de la Inteligencia Artificial en las elecciones refuerzan la prohibición de la IA. Documento de trabajo, 2024. Available at: [https://paperswithcode.com/paper/deceptive-uses-of-artificial-intelligence-in#:~:text=We%20propose%20a%20framework%20for%20assessing%20AI's%20impact%20on%20elections]. Consulted: 30.09.2024.
KAVANAGH, J.; RICH, M. D. La decadencia de la verdad. Una exploración inicial del papel decreciente de los hechos y el análisis en la vida pública estadounidense. Sacramento: Rand Corporation, 2018.
KERTYSOVA, K. Inteligencia artificial y desinformación: cómo la IA cambia la forma en que se produce, se difunde y se puede contrarrestar la desinformación. Seguridad y Derechos Humanos, vol. 29, 2018, pp. 55-81.
FUNDACIÓN KOFFI ANNAN. PROTEGER LA INTEGRIDAD ELECTORAL EN LA ERA DIGITAL. INFORME DE LA COMISIÓN KOFI ANNAN SOBRE LAS ELECCIONES EN LA ERA DIGITAL. GINEBRA: KAF, 2020.
KOLB, Andrew. Elections in Kenya. IFES Annual Report 2022. Available at: [https://www.ifes.org/ifes-annual-report-2022/elections-kenya]. Consulted: 29.10.2024.
KREPS, S.; KRINER, D. Cómo amenaza la IA a la democracia. Journal of Democracy, v. 34, Issue 4, October 2023, pp. 122-131.
LESSIG, L. The law of the horse: what cyberlaw might teach. Harvard Law Review, v. 113, 1999, pp. 501-546.
LEVITIN, D. LA MENTIRA COMO ARMA POLÍTICA. MADRID: ALIANZA EDITORIAL, 2019.
LIMA-STRONG, C. Todos los principales proyectos de ley tecnológicos firmados y vetados por el gobernador de California. The Washington Post, 1 de octubre de 2004. Available at: [https://www.washingtonpost.com/politics/2024/10/01/all-major-tech-bills-californias-governor-signed-vetoed/]. Consulted: 21.10.2024.
LISSANU, A.; MORAGA, P.; SOBOL, I. Plataformas mediáticas, expresión y derechos humanos. Global Constitutionalism Seminar 2024, Yale Law School, September, 2024, pp. 37-52.
LÓPEZ PONCE, J. TEPJF ofrecerá inteligencia artificial para asesorar dictámenes electorales. Milenio, June 18, 2024. Available at: [https://www.milenio.com/politica/tribunal-electoral-ofrecera-ia-juicios-electorales]. Consulted: 08.10.2024.
LOZANO, I. Son molinos, no gigantes. Cómo las redes sociales y la desinformación amenazan nuestra democracia. Barcelona: Península, 2020.
MACHADO, R. C. R.; PORTELLA, L. C. Inteligencia artificial, elecciones y autenticidad electoral. En: SILVEIRA, M. de P. Elecciones y nuevas tecnologías. Datos, inteligencia artificial y (des)información. Brasília: Ethics 4AI; Instituto Brasiliense de Direito Público, 2024, pp. 573-588.
MAINZ, J. T; SØNDERHOLM, J.; UHRENFELDT, R. Artificial intelligence and the secret ballot. AI and Society, v. 39, 2022, pp. 515-522.
MARTINEZ-BRAWLEY, E. E. Hatespeech. A bird's eye view of a conundrum of international epidemic proportions. En: GUALDA, E. Teorías de la conspiración y discurso del odio online en la sociedad de plataformas. Comparación de agendas en narrativas y redes sociales sobre Covid-19, inmigrantes, refugiados, estudios de género y personas LGBTQ+. Madrid: Dykinson, 2024, pp. 43-59.

MATORUGA, E. El papel de la AI en la lucha contra las operaciones de influencia encubierta. Available at: [https://www.hulkapps.com/es/blogs/ecommerce-hub/el-papel-de-la-ia-en-la-lucha-contra-las-operaciones-de-influencia-encubierta]. Consulted: 08.10.2024.

MEIRINHO MARTINS, M. Representação política. Elecciones y sistemas electorales: una introducción. 2. ed. Lisboa: Instituto Superior de Ciências Sociais e Políticas, 2015.

MOSERO, Rose. In Kenya's 2022 Elections, Technology and Data Protection Must Go Hand-in-Hand. Available at: [https://carnegieendowment.org/research/2022/08/in-kenyas-2022-elections-technology-and-data-protection-must-go-hand-in-hand?lang=en]. Consulted: 29.10.2024.

MUÑOZ, K. El año electoral de la IA: cómo contener el impacto de la inteligencia artificial. DGAP Memo, No.1, 2024, pp. 1-5.

NORDEN, L.; NARANG, N; PROTZMANN, L. J. States Take the Lead in Regulation AI in Elections - Within Limits. Centro Brennan para la Justicia, August 7, 2024. Available at: [https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits]. Consulted: 20.10.2024.

NUNES, F.; TRAUMANN, T. Biografía del abismo. Cómo la polarización divide a las familias, desafía a las empresas y pone en peligro el futuro de Brasil. Río de Janeiro: Harper Collins, 2023.

OGWUCHE, C.; ONAH, C. Behavioural Manipulation, Regulations and Oversight of Artificial Intelligence (AI) in Political Campaigns and Elections in Nigeria. Nigerian Psychological Association, Congreso Nacional, August, 2023. Available at: [https://www.researchgate.net/publication/380403967_Behavioural_Manipulation_Regulations_and_Oversight_of_Artificial_Intelligence_AI_in_Political_Campaigns_and_Elections_in_Nigeria]. Consulted: 18.10.2024.

OKOYE, F. Tackling Nigeria's Electoral Challenges Utilising AI. This Day, October 22, 2024. Available at: [https://www.thisdaylive.com/index.php/2024/10/22/tackling-nigerias-electoral-challenges-utilising-ai/]. Consulted: 23.10.2024.

OLIVA, T. D.; TAVARES, V. P; VALENTE, M. ¿Una solución única para toda Internet? Diagnósticos y Recomendaciones, No. 4, septiembre de 2020. Available at: [https://www.internetlab.org.br/wp-content/uploads/2020/09/policy_plataformas-conhecimento_20200910.pdf]. Consulted: 26.09.2024.

OSCE (Organization for Security and Co-operation in Europe). OSCE and Ukraine-s Central Election Comission launch chatbot to ease access to information in advance of 25 October local elections. Available at: [https://www.osce.org/project-coordinator-in-ukraine/466011]. Consulted: 23.10.2024.

PANDITHARATNE, M.; GIANSIRACUSA, N. Cómo la inteligencia artificial pone en riesgo las elecciones y las medidas que se requieren para protegernos. Brennan Center, July 13, 2023. Available at: [https://www.brennancenter.org/es/our-work/analysis-opinion/inteligencia-artificial-pone-en-riesgo-elecciones-medidas-proteger-democracia]. Consulted: 03.10.2024.

PENAGOS RAMÍREZ, Juan Pablo. Registraduría revela cómo usará la inteligencia artificial para sistema de identificación y electoral de los colombianos. El Tiempo, August 26, 2024. Available at: [https://www.eltiempo.com/politica/partidos-politicos/registraduria-revela-como-usara-la-inteligencia-artificial-para-sistema-de-identificacion-y-electoral-de-los-colombianos-3375089]. Consulted: 23.10.2024.

PÉREZ DE LAMA, J.; SÁNCHEZ-LAULHÉ, J. Consideraciones a favor de un uso más amplio del término tecnopolítica. Sobre la necesidad de la crítica y la política del conocimiento tecnológico. En: SABARIEGO, J.; AMARAL, A. J.; SALLES, E. B. C. (Coords.). Algoritmos. Valencia: Tirant lo Blanch, 2020, pp.19-43.

RAMONET, I. LA ERA DEL CONSPIRACIONISMO. TRUMP, EL CULTO A LA MENTIRA Y EL ASALTO AL CAPITOLIO. BUENOS AIRES: SIGLO XXI, 2022.

ROTARU, G.; ANAGNOSTE, S; OANCEA, V. How Artificial Intelligence can influence elections: analysing the large language models (LLMs) political bias. Actas de la 18ª Conferencia Internacional sobre Excelencia Empresarial 2024, pp. 1-10.

RUBIO NÚÑEZ, Rafael; ALVIM, Frederico Franco; MONTEIRO, Vitor de Andrade. Inteligencia artificial y campañas electorales algorítmicas: Disfunciones informativas y amenazas sistémicas de la nueva comunicación política. Madrid: CEPC, 2024.

RUBIO NÚÑEZ, Rafael; MONTEIRO, Vitor de Andrade. Preserving trust in democracy: The Brazilian Superior Electoral Court's quest to tackle disinformation in elections. South African Journal of International Affairs. 30. 1-24. 2024. DOI 10.1080/10220461.2023.2274860.

SAFIULLAH, M.; PARVEEN, N. Big Data, Artificial Intelligence and Machine Learning: a paradigm shift in election campaigning. The New Advanced Society, 2021, pp. 247-261.

SÁNCHEZ MUÑOZ, O. LA REGULACIÓN DE LAS CAMPAÑAS ELECTORALES EN LA ERA DIGITAL. DESINFORMACIÓN Y MICROSEGMENTACIÓN EN REDES SOCIALES CON FINES ELECTORALES. MADRID: CENTRO DE ESTUDIOS POLÍTICOS Y CONSTITUCIONALES, 2020.

SANDEL, M J. El descontento de la democracia. Un nuevo enfoque para tiempos peligrosos. Río de Janeiro: Civilización Brasileña, 2023.

SAPADA, A. T.; ARIF, M. Use of Artificial Intelligence in General Elections: Comparison of Indonesian and German Regulations. Law and Social Journal, vol. 1, No. 1, 2024, pp. 21-40.

GOBIERNO DE SINGAPUR. Nuevas medidas legales para mantener la integridad de la publicidad en línea durante las elecciones. Ministerio de Desarrollo Digital e Información, September 9, 2024. Available at: [https://www.mddi.gov.sg/new-legal-measures-to-uphold-integrity-of-online-advertising-during-elections/]. Consulted: 21.10.2024.

SOON, C.; QUEK, S. Salvaguardar las elecciones de las amenazas de la inteligencia artificial. IPS Working Papers, No. 56, August, 2024.

SUÁREZ, P. S. La inteligencia artificial (AI) y las elecciones: breves y primeras reflexiones sobre el uso, el impacto y la influencia de la AI en los procesos electorales. Pensar en Derecho, No. 22, 2023, pp. 33-51.

TAVARES, A. R. El riesgo democrático en la era digital. En: BRANCO, P. G. G; FONSECA, R. S. da; BRANCO, P. H. de M. G; VELLOSO, J. C. B.; FONSECA, G. C. S. Eleições e democracia na era digital. São Paulo: Almedina, 2022, p. 427-438.

TAVARES, C. de M. Inteligência artificial e deepfakes: desafios jurídicos e tecnológicos para a integridade do processo democrático e implicações para as eleições municipais de 2024. Justiça Eleitoral em Debate, v. 14, No. 1, 2024, pp. 49-58.TOMIĆ, Z.; DAMNJANOVIĆ, T.; TOMIĆ, I. Artificial Intelligence in Political Campaigns. South Eastern European Journal of Communication, vol. 5, No. 2, Winter 2023, pp. 17-28.

TUSET VARELA, Damián. Cuando la IA decide: fronteras legales y éticas de la IA em el sistema electoral. Diario La Ley, February 2, 2024. Available at: [https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAC2NwWrDQAxEv6Z7MRQ3PqQ97MX1MZTSmt5lWdgLm1Uqad347yuSCAaN0Ejvt5LsI10tIhcTzo0yJshNTpNQg0mwZsDEpbmQKBfQoHvhsp_jKJWCwaSxfTrii-sQAK1CHhjjzaeNRphiG1hmkn53Z2yQv0hj1x6Drvz3AVtawBzRg9yfpnmOw9h6dW_d4bULm7M9EH_SQsUorGlZTy6755VAcP2EhaKj69kz_Ax6uT42fTXz68nK920OmL0PYPQOmcr84P4DslXoVw0BAAA=WKE]. Consulted: 23.10.2024.

SLOWING-ROMERO, S.; SCRIVEN, J. Democracia, retroceso y tribunales. Global Constitutionalism Seminar 2024, Yale Law School, September, 2024, pp. 3-18.

SOUZA NETO, C. P. DE. DEMOCRACIA EN CRISIS EN BRASIL. SÃO PAULO: CONTRACORRENTE, 2020.

STEVENSON, K. Inteligencia Artificial: un arma de doble filo en las elecciones. Educational Administration: Theory and Practice, 30(4), 2024, pp. 1.660-1.667.
SULEYMAN, M.; BHASKAR, M. The next wave: artificial intelligence, power and the greatest dilemma of the 21st century. Río de Janeiro: Record, 2024.
Gobierno británico. A pro-innovation approach to AI regulation. Policy Paper, August 3, 2023. Available at: [https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper]. Consulted: October 21, 2024.
UNDP (United Nations Development Programmes). Election Comission uses artificial intelligence to enhance women's participation in electoral processes, August 9, 2022. Available at: [https://www.undp.org/libya/press-releases/election-commission-uses-artificial-intelligence-enhance-womens-participation-electoral-processes]. Consulted: 23.10.2024.
UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura). Elecciones en la era digital. Guía para profesionales electorales. Available at: [https://unesdoc.unesco.org/ark:/48223/pf0000382102]. Consulted: 21.08.2024.
VALDES ZEPEDA, A.; ARÉCHIGA, D.; DAZA MARCO, T. Inteligencia artificial y su uso en las campañas electorales en sistemas democráticos. Revista Venezolana de Gerencia, Año 29, No. 105, 2024, pp. 63-76.
VESTING, T. El cambio de la esfera pública por la inteligencia artificial. En: ABBOUD, G.; NEY JR., N.; CAMPOS, R. (eds.). Fake News y regulación. 2. ed. São Paulo: RT, 2020, pp. 193-210.
VIVAS ESCRIBANO, G. Desinformación y polarización en relación con las redes sociales. En: CARRATALÁ, A.; IRANZO CABRERA, M.; LÓPEZ GARCÍA, G. (eds.). De la desinformación a la conspiración. Política y comunicación en un paisaje mediático híbrido. Valencia: Tirant lo Blanch, 2023, p. 351-359.
VLACHOS, S. The link between mis-, dis-, and malinformation and domestic extremism. Consejo de Asuntos Emergentes de Seguridad Nacional, June, 2022. Available at: [MDM_22.6.17b.pdf (censa.net)]. Consulted: 30.08.2024.
CASA BLANCA. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Available at: [https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/]. Consulted: 21.10.2024.
FORO ECONÓMICO MUNDIAL. Informe sobre Riesgos Mundiales 2024: Insight Report, 19ª edición. January, 2024.
YAZBEK, S. Inteligencia artificial aplicada a los procesos electorales. Instituto Democracia y Elecciones, April 27, 2024. Available at: [https://idemoe.org/la-inteligencia-artificial-aplicada-a-procesos-electorales-desafios-de-la-observacion-electoral/]. Consulted: 03.10.2024.
YU, C. ¿Cómo nos robará la IA las elecciones? Centro para la Ciencia Abierta, OSF Preprints, 2024, pp. 01-24.
ZACHARY, G. P. Digital manipulation and the future of Electoral democracy in U.S. IEEE Transactions on Technology and Society, v. 1, No. 2, June 2020, pp. 104-112.