UDK 324:316.774
DOI https://doi.org/10.2298/FID2502387P
Original Scientific Article
Received 06.06.2024. Accepted 12.03.2025.

PHILOSOPHY AND SOCIETY
VOL. 36, NO. 2, 333–572

To cite text:
Parenteau, Ian. 2025. "Navigating the Limits: Electoral Management Bodies and the Struggle Against Disinformation and Foreign Interference." *Philosophy and Society* 36 (2): 387–412.

Ian Parenteau

NAVIGATING THE LIMITS: ELECTORAL MANAGEMENT BODIES AND THE STRUGGLE AGAINST DISINFORMATION AND FOREIGN INTERFERENCE

ABSTRACT
The problem of disinformation and foreign interference in elections has increased significantly in recent years. It creates an uneven playing field that hinders fair competition and informed voting. Electoral disinformation manifests itself in two ways: partisan and procedural. Partisan disinformation targets candidates and voters with false information to influence their voting preferences. In contrast, procedural disinformation seeks to disenfranchise voters or undermine the electoral process. Foreign interference in elections can be defined as any attempt to influence the outcome of an election in another country. Have Electoral Management Bodies (EMBs) implemented effective countermeasures to mitigate these risks? The answer is complex, but no. They face institutional, legal and technical constraints that limit their actions. First, EMBs cannot change electoral laws to make them more resilient against the threat of disinformation and foreign electoral interference. Second, disinformation is usually not criminal and falls outside most legislation, making prosecution difficult. Foreign interference falls beyond national jurisdiction. Third, the actions that EMBs can take are limited by their obligations to be fair and impartial. Fourth, while enhancing content curation on social media platforms would be beneficial, EMBs lack the authority to enforce such measures, and these platforms exercise limited control over the content that is published.

KEYWORDS
Electoral Management Bodies (EMB), disinformation, foreign electoral interference, and elections.

Introduction

Electors are increasingly exposed to new risks that can undermine the integrity of free and fair elections. Until a decade ago, electoral malpractice mostly took the shape of vote buying, and harassment of voters, candidates and electoral staff to attempt to manipulate results. The enactment of more robust electoral laws and the professionalization of Electoral Management Bodies (EMB)

Ian Parenteau: Assistant Professor, Departement of Humanities and Social Sciences, Collège militaire royal de Saint-Jean, Québec, Canada; ian.parenteau@cmrsj-rmcsj.ca

have gone a long way towards eliminating these risks and making elections safe. Nonetheless, these measures appear to provide a frail defence against new electoral risks. Disinformation and foreign interference, both phenomena that have escalated dramatically over the last few years, greatly distort the level playing field that allows candidates to compete fairly and voters to make informed choices. They are a growing threat to electoral integrity in all democracies. Recent electoral events give abundant examples of the scale of this problem[1].

In order to mitigate new electoral risks, some national security agencies have adopted a deterrence defence strategy. In October 2017, the German Parliament enacted the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*) to curb the dissemination of disinformation and hate speech[2]. In January 2019, the government of Canada established the Critical Election Incident Public Protocol (CEIPP) to inform citizens of a threat to the integrity of elections (Democratic Institutions 2020). France established the digital security agency VIGINUM in July 2021 to safeguard against digital foreign interference[3]. The US Justice Department has implemented measures to disrupt foreign malign influence operations (US Justice Department 2024). The Australian Government recently launched the security initiative "Countering Foreign Interference in Australia: Working together towards a more secure Australia" in order to reduce this threat (Department of Home Affairs 2024).

Some EMBs, such as in Estonia, Australia and Canada have also taken steps to secure the right to vote and, in particular, to limit the spread of disinformation. Even so, as this article will explore, when examining EMBs' action plans, a pressing question arises: despite the seriousness of the new electoral risks, why have electoral administrators implemented only a limited set of countermeasures so far? We argue that this shortcoming arises because all mitigation efforts are constrained by a complex set of institutional, legal, and technical limitations, which restrict the scope of action available to all stakeholders in this fight—most notably EMBs themselves. Consequently, while EMBs strive

1 For a comprehensive overview of foreign information manipulation and interference in elections, see O'Connor, Sarah, Fergus Hanson, Emilia Currey, and Tracy Beattie (2020), "Cyber-enabled foreign interference in elections and referendums," *International Cyber Policy Centre at ASPI* 63. For recent disinformation campaign overview per country, see EU DisinfoLab publications at https://www.disinfo.eu/publications.

2 The *Netzwerkdurchsetzungsgesetz* (NetzDG) law is designed to limit the spread of disinformation and hate content on social networks. It came into force on October 1, 2017. The Law obliges for-profit social networks to remove plain hateful content within 24 hours of being reported. If the illegal nature of the content is less obvious, the networks have a week to react. See https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

3 Set up in July 2021, VIGINUM's mission is to detect and characterize any suspicious propagation of misleading or hostile content on digital platforms involving foreign actors intending to harm France and its interests. See: https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques

to implement safeguards against these risks, they often find themselves unable to overcome this complex and multifaceted impasse. Furthermore, although the study of electoral disinformation is well established, the distinction between partisan and procedural disinformation remains unclear, hindering EMBs' ability to effectively address the unique challenges posed by this threat.

Before proceeding with our analysis, three important remarks must be highlighted. First, EMBs enjoy varying degrees of autonomy, which limits any general conclusions we may draw. For instance, comparing mixed model EMBs in France and Spain with fully independent EMBs in Canada, Estonia and Costa Rica would be inaccurate and misleading. The latter have broad powers, allowing them to intervene with voters, candidates, and election officials before and after writs are issued. In contrast, the former only have responsibilities for conducting elections. Hence, each EMB should be evaluated on its own terms, so we can only offer a preliminary assessment at this stage. A more in-depth examination of each EMB would be necessary, but it falls outside the scope of this article. Second, it's essential to recognize that EMBs alone cannot bear the entire responsibility for countering election-related hazards. Other national security actors also play a role in this effort, making it unfair to place the full burden of responsibility on EMBs for any shortcomings in the defence against such threats. Third, disinformation in other non-electoral related fields, such as vaccination against COVID-19 (Sessa 2022a), the Russian invasion of Ukraine (Sessa 2022b), climate change (Dave, Ndulue, and Schwartz-Henderson 2020), and Brexit (Marshall and Drieschova 2018), also constitute a real struggle against which the scientific, public health, and national security communities, despite their efforts, have yet been able to develop an effective defence. Therefore, it would be wholly unrealistic to expect EMBs to single-handedly address the threat of electoral disinformation. Keeping these limitations in mind, our examination of EMB actions will be shaped accordingly.

This article is divided into four sections. The first section distinguishes between partisan and procedural disinformation and defines foreign interference in elections. The second section reviews the risk mitigating strategies that EMBs have adopted. The third addresses our research question and thus examines four key limitations that they face in safeguarding elections. Finally, the fourth section outlines potential strategies that EMBs could adopt to preserve electoral integrity, followed by our conclusion.

What Is Disinformation?

Disinformation is "[i]nformation that is false and deliberately created to harm a person, social group, organization or country" (Wardle and Derakhshan 2017:20). In the context of an election, disinformation aims to influence either public opinion in general, to undermine the sincerity of the vote or, more specifically, a group of electors in an attempt to alter their voting preferences and behaviour. Disinformation producers and disseminators use various technical and communication strategies. They can spread false or misleading stories and

credit distorted statements to a candidate to erode his credibility and arouse disapproval. They can publish online images and videos edited by software, such as Deep Fakes (Garnett and Pal 2022; Łabuz and Nehring 2024). They may exploit coordinated, inauthentic online behaviour with the same goal by feeding several fake social media profiles. To bolster a candidate's popularity, they may resort to *astroturfing* – wrongfully implying that a successful event is of spontaneous citizen origin (Boulay 2015). The disinformation *modus operandi* also involves nourishing trolls by stoking online debates on divisive topics with false or partially fabricated information (Clucas 2020). Disinformation also circulates on fake sites, whose authors resort to "typosquatting" - the practice of producing counterfeit articles on a page identical in every respect to those on the official site of well-established media but with a different domain name that resembles the original (Irish 2023). The range of techniques used to disseminate disinformation is constantly expanding, thanks in particular to the new capabilities offered by artificial intelligence (Helmus 2022). Social media platforms, such as Facebook, X, WhatsApp, TikTok, WeChat and Telegram, are the main disinformation vectors. It circulates there abundantly due to the ease with which anyone can use this digital space. Platforms also implement techniques such as microtargeting (Crain and Nadler 2019; Kusche 2019), which consists of personalizing users' content based on the fine segmentation of their online behaviours and the wide operationalization of recommendation algorithms (Pariser 2012). This further accentuates online fragmentation facilitating disinformation efforts.

Although disinformation bears numerous causes that are no doubt linked to today's geopolitical tensions (Rosenbach and Mansted 2019), it is also one of the main consequences of the business model of digital platforms, which entirely rests on user engagement – engagement that platforms can subsequently monetize by the sale of advertising (Brown 2021). Disinformation circulates as much in public and semi-public spaces of digital platforms – as in a post, video or message published for online friends (or the public, depending on privacy settings). As the web is borderless, actors involved in disinformation campaigns can run from any country. Sometimes, traditional print media and broadcast media can also contribute to spreading disinformation by publishing articles with misleading claims. This is the case, for example, of the Russian state-funded media RT and Sputnik, which the European Union banned following Russia's invasion of Ukraine in February 2022 because Brussels suspected them of "systematic information manipulation and disinformation" (Union européenne 2022).

The Two Types of Electoral Disinformation

Electoral contests are a host of two types of disinformation. *Partisan disinformation*, by far the most frequent form, aims to manipulate public opinion to influence voters' choices. It targets candidates, political parties and citizens. Examples during recent elections, in both stable and emergent democracies,

are almost infinite (ADF 2023; Jalli 2023; Osborn 2023). The perpetrators employ the panoply of ruses listed above to reduce the electoral fortunes of selected candidates. They may also be explicitly aimed at driving electoral abstention among voters who have shown their support for a candidate or who are inclined to do so given their socio-economic profile – the latest research in electoral sociology has illustrated, for instance, that better-educated voters tend to back left-wing parties (Gethin, Martínez-Toledano, and Piketty 2021).

Procedural disinformation, the second type, targets electoral administrations, political parties and voters (Boston Globe, 2022). It consists of circulating false information about voting procedures, such as polling station opening hours, documents electors must present to vote or the list of candidates to damage the credibility of election results. Procedural disinformation primarily aims to disenfranchise certain voters to reap electoral gains. It could also be used to question the sincerity of the election or the conditions under which the ballot is held, as the outcome looks unlikely to be favourable to the candidates of their choice. As in the case of the 2016 US presidential elections, it can also harbour the ambition of undermining social cohesion by promoting divisive issues such as race, LGBT rights, and immigration. These are just some of the many goals of this type of disinformation. Sometimes, its true motivations are complex, as the sole purpose seems to be making as much noise as possible (Gessen 2018). For example, during Brazil's 2018 presidential elections, the Tribunal Superior Eleitoral (TSE) was the target of a disinformation campaign on X that suggested that the electronic ballot boxes had been hacked (Recuero 2020; Taboada et al. 2023). During the Tunisian presidential elections in October 2019, opponents of Salma Elloumi's candidacy circulated the information that she had withdrawn in favour of another candidate in an attempt to influence voters' choices (Business News 2019). During the 2021 US presidential elections, false information was abundantly relayed on social networks concerning postal voting to restrict the participation of voters deemed more inclined to use this voting device (Censky 2021; Qiu 2021). These examples show the variety of strategies malevolent actors can exploit in a bid to make electoral gains or try to breed mistrust in the electoral process.

Procedural disinformation thus represents a key concern in that it can undermine the smooth running of elections, regardless of the impact it may have on voters' choices – the effect linked to partisan disinformation. The primary mandate of EMBs is to organize elections in full compliance with the provisions of the electoral law and other legal and administrative constraints to which they are subject. What's more, EMBs have little control over the conditions under which voters make their electoral choices. For example, they cannot influence the quality of information provided to voters by candidates. On the other hand, at least a majority of EMBs are responsible for controlling factual information about voting procedures. This is why fighting this type of disinformation matters for EMBs.

What Is Foreign Electoral Interference?

Foreign election interference campaigns pursue similar aims, using partisan and procedural disinformation as their main informational component (Jeangène Vilmer et al. 2018; Mohan and Wall 2019; Schmitt 2021; Tenove et al. 2018). They also use other means, chiefly illicit, to gain influence over the verdict of the ballot box. By hacking into the computer systems of electoral administrations and political parties, foreign agents can try to change electoral data – by making certain votes disappear or altering election results. They may set out to make computer systems inaccessible by conducting distributed denial-of-service (DDoS) attacks or phishing attempts to disrupt the computer infrastructure and services of EMBs. Estonia was the subject of a cyber-attack during the parliamentary elections of March 2023 (Martin 2023). In 2023, hackers managed to gain entry via a very sophisticated attack on the electoral registers of the UK Electoral Commission (Seddon 2023). During the 2019 Kosovar parliamentary elections, the online election results display systems also suffered a major denial-of-service attack from Russia (Ahmetaj 2021). Hackers can try to influence voters' opinions by making public information about candidates they allegedly stole. This was the case during the 2017 French presidential elections when Emmanuel Macron's campaign team fell victim to leaked emails (Vilmer 2019). Foreign interference can also be motivated by an attempt to discredit the electoral process by relaying the rumour that the electoral outcome has been doctored. More traditionally, it can take the form of financial support for a candidate or political party or harassment of a candidate or family members (Hogue 2024; Zimonjic 2024).

Measures EMBs Have Adopted to Mitigate New Electoral Risks

In face of the growing menace of new electoral risks, some EMBs have adopted risk mitigating measures. In 2016, Valimised, the Estonian State Electoral Office, created an inter-agency task force to safeguard against disinformation (McBrien 2020). In 2018, the Australian Electoral Commission put together the Electoral Integrity Task Force, a year-round multistakeholder team, which includes police and intelligence services, whose objective is to protect the integrity of electoral processes (Australian Electoral Commission 2018). AEC also implemented the Disinformation Register, which "lists prominent pieces of disinformation the AEC has discovered regarding the electoral process"(Australian Electoral Commission 2023b). Since March 2020, The Electoral Service of Chile (Servicio Electoral) offers electors a fact-checking page with an electoral "Fake news repository." In 2021, the German Federal Returning Officer launched a similar fact-checking service on its sites (Die Bundeswahlleiterin 2021). In November 2021, participants at the XV Conference of the Inter-American Union of Electoral Bodies (Uniore) set up the Inter-American Observatory for Combating Disinformation, whose function is to build strategic alliances with fact-checking agencies and social media platforms (OICDE

2022). In 2022, before the regional and municipal elections, Peru's National Elections Jury (JNE) and the National Office of Electoral Processes (ONPE) implemented a bot service on WhatsApp to provide information about voting, such as polling places, to fight electoral disinformation (Oficina Nacional de Procesos Electorales 2022). They also added a fact-checking component to the channel with the support of a fact-checking initiative called ONPEChequea (ONPEChequea 2022). In June 2022, Brazil developed the Electoral Disinformation Alert System (SIADE), designed to facilitate the detection and prompt response to false content that could influence the electoral process (Tribunal Superior Eleitoral 2022).

After the 2022 federal election, AEC implemented a Reputation Management System (RMS), an institutional-wide approach to maintain voters' confidence in electoral integrity (Australian Electoral Commission 2023a:6). In October 2023, the Electoral Tribunal of Panama (TE) developed a fact-checking service on its website called "VerificadoContigo" (*verified with you*)[4]. In 2023, Elections BC from Canada implemented a Disinformation Register on its website, which lists prominent falsehoods or misperceptions that have come to their attention (Elections BC 2024). In 2023, the Parliament of British Columbia updated its Electoral Law to make it illegal to transmit false statements about candidates' citizenship and profession, as it might influence electoral outcomes (Legislative Assembly of British Columbia 2023). In January 2024, Elections Canada launched the "ElectoFacts", a tool designed to inform voters during the next federal elections (Elections Canada 2024). Élections Québec's latest strategic plan includes the objective of preventing the use of disinformation in electoral contexts by improving their preparedness, reducing the public's vulnerability to electoral disinformation, increasing transparency and access to data, and preventing the use of disinformation in electoral contexts (Élections Québec 2024:20). The Élections Québec website also provides a section on the various types of disinformation and how to handle them if encountered (Élections Québec 2021). The 2024-28 Elections Alberta's strategic plan included developing a communication plan to emphasize "transparency within legislative limits, combating misinformation and disinformation, and creating safe spaces for public discourse" (Elections Alberta 2023:29).

In 2020, Anton Boegmen, Elections BC CEO, recommended that more robust changes impose restrictions on electoral advertising, limit electoral financial contributions to Canadian residents only, and regulate social media platforms, but those have yet to be implemented (Boegman 2020). Pierre Reid, CEO of Élections Québec, also proposed legislative changes in 2023 to require social media platforms to register election-related advertising and to add new offences specifically addressing disinformation in the Election Act to more effectively combat information manipulation (Élections Québec 2023:119).

4 https://verificadocontigo.com/

Why Have EMBs Adopted Insufficient Risk Mitigating Measures?

EMBs have Limited Legislative Power

While the initiatives proposed by EMBs may enhance election security, assessing their effectiveness remains challenging, as they are difficult to evaluate outside the context of an actual election. More importantly, despite the significant threats facing voters, the proposed measures appear both insufficient and overly cautious, as this overview demonstrates—they simply do not match the scale of the threat. Why have EMBs adopted only a limited set of timid risk-mitigation measures? The first reason for this is that most EMBs operate within rigid legal frameworks, making it difficult for them to proactively address threats such as cyber-attacks, disinformation, and new forms of voter suppression. They lack the ability to push for necessary legislative updates, which greatly limits their capacity to implement essential reforms. Even those classified as independent and considered a "fourth branch of government" by Michael Pal (Pal 2016:2) lack the plenary powers to amend legislation to make it more robust against new electoral risks. In the brief history of electoral administrations, which has not yet celebrated its hundredth anniversary, the primary concern for EMBs has been the potential for partisan capture. This is why, little by little, democratic countries have adopted constitutional safeguards to ensure that EMBs can hold fair and free elections, in other words, in a non-partisan manner. This protection allows most EMBs to set electoral rules and guidelines, which any other branch of government cannot revise, let alone elected officials, as long as they comply with the constitution and electoral laws. They have limited executive powers to call and hold elections, certify or annul election results, and resolve electoral disputes. They can impose fines on offenders, particularly in the area of the financing of political parties and candidates. Some electoral administrations may also set the date of the ballot, provided that they comply with the parameters set by the electoral law relating to the length of terms of office, for example.

On the other hand, Members of Parliament (MPs) determine the roles and responsibilities of EMBs. They allocate EMB's budget, appoint their members and set their terms and conditions of employment. For instance, the eight members of the Electoral Commission of Jamaica are Selected and Nominated by both the Prime Minister and the Leader of the Opposition (Ministry of Justice of Jamaica 2006). In Mexico, Members of the Instituto Nacional Electoral (INE) are appointed by a two-third vote by parliamentarians (INE 2017). Because of this constitutional framework, EMBs do not exercise plenary powers to amend laws in several areas linked to national security, which is entirely natural. Still, overall they cannot initiate reforms related to registering and voting regulations, nor the conditions under which ballots are cast[5]. For instance,

5 This is true for reforms that are considered minor, major, and technical based on the distinction established by Kristof Jacobs and Monique Leyenaar. See (Jacobs and Leyenaar 2011)

Germany's Federal Returning Officer cannot amend the federal electoral law, as the Federal Ministry of the Interior and Community is the sole authority (Die Bundeswahlleiterin 2024). Nor can the Electoral Commission of the UK reform the Electoral law (The Electoral Commission 2023:8). France's electoral legislative framework can only be amended by the National Assembly and the Senate once it has been deemed to comply with the Constitution by the Constitutional Council (Vie publique 2021). Similarly, the newly established Electoral Commission of Ireland's power is limited to "advice and make recommendations to the Government or the Minister, about any proposals for legislative change, or any other policy matters concerning electoral policy or procedures," when and only when "requested by the Minister," (The Electoral Commission 2024). The Republic of Korea is a very rare exception to this rule, as, since 1992, the National Election Commission (NEC) can "submit a bill to the National Assembly when it is necessary to enact a new law or amend an existing law concerning elections," as can do any other ministry (Kim 2024). Similarly, the South African Constitution grants the Electoral Commission the power to "continuously review electoral legislation and proposed electoral legislation, and to make recommendations in connection therewith" (South African Government 1996:2). However, although these EMBs have more power, they still need to convince MPs to adopt new election laws to enhance their resilience to new electoral risks.

However, history tells us that MPs have been known to ignore such recommendations, as partisan interests often influence their decisions. As Kenneth Benoit has shown in his research on electoral reforms, once elected, representatives of the majority party usually prefer the status quo and are unlikely to support any proposed amendments to the electoral law unless they believe it will help them win more seats in the next election (Benoit 2004). Even when most citizens favour a legislative change, such as eliminating the first-past-the-post electoral system in Canada, ruling political parties have chosen to maintain the existing system because they consider it more advantageous (Lajoie 2022; Thompson 2022). Consequently, proposals to amend electoral laws to counter disinformation and foreign interference are most often met with inertia. As a result, EMBs limited legislative competence hinders their capacity to adopt robust measures against new electoral risks (Vallée 2023).

Disinformation Very Rarely Constitutes a Criminal Act

The second reason for EMBs' limited action is that, like all other stakeholders fighting disinformation and foreign interference, they face serious legal restrictions. Disinformation rarely constitutes an illegal act (Gill 2020:14), and foreign interference can hardly ever be prosecuted.

In general, criminal law in any democratic society is guided by three basic principles: i) any action that constitutes a crime must be clearly defined; ii) after a trial, a guilty verdict must be accompanied by a sentencing decision; and iii), the means of enforcing this decision must be within the reach of the

authorities. In disinformation cases, point i) presents the most significant difficulties; in the case of foreign interference, point iii) poses a challenge.

Disinformation must be illegal for it to be considered a crime. Very few laws expressly prohibit it, which we will discuss below. However, there exist certain legal provisions that criminalize activities that could amount to disinformation using current categories of illegal content, but as we will see, they have a limited impact on reducing this phenomenon. For instance, in Canada, hate speech is considered a crime if it causes harm and "undermines the dignity of others" (Supreme Court of Canada 2013). The legal threshold for a verdict of culpability is very high, as any democratic society values freedom of expression and thus must accept "some competition in the marketplace of ideas" (Sharpe 1987:232). Sharing a message on social media that falsely attributes a quote to a candidate or puts it out of context does not contravene hate speech provisions (Walker 2018). Nor does circulating the idea that candidate Emmanuel Macron's election campaign during the 2017 presidential elections was financed by Saudi Arabia (Feertchak 2017). From this point of view, it is simply not a crime. In April 2024, Scotland revised its *Hate Crime and Public Order Act* to enhance protection against discriminatory acts targeting individuals based on disability, race, religion, sexual orientation and gender identity. However, this amendment has a minimal impact on disinformation, as it does "not prevent people expressing controversial, challenging or offensive views" (Scottish Government 2024). Despite the recent amendment to this law, disinformation remains largely unregulated in Scotland.

In the same vein, one might also be inclined to use laws against defamation, as disinformation might resemble this, and lawsuits of this kind might come more easily to fruition. The crime of disinformation would then be considered a kind of defamation. However, as Lili Levi has demonstrated, legal actions for defamation have limited effectiveness in combating disinformation. They often fail to uncover the underlying truths beyond the specific statements in question and instead focus on providing redress to those who have suffered injustice. (Levi 2022). Consequently, such laws have also a limited impact on disinformation.

Lastly, disinformation might approximate false advertising. For instance, Canada's Competition Act contains provisions addressing "false or misleading representations and deceptive marketing practices in promoting the supply or use of a product or any business interest" (Government of Canada 1986:74.011). In this case, the main limitation is that disinformation is not usually aimed at selling a product or service. Rather, it is about intentionally disseminating false information. This approach would be ineffective in addressing disinformation, as it fails to acknowledge it as a criminal act and therefore fails to stop its spread.

That said, some electoral laws prohibit the spread of false information. Legislators from different countries have taken three different approaches. One approach treats disinformation as a "content-related crime" and bans specific types of untrue information and content from being shared. Another approach considers disinformation as a "consequential crime" and evaluates it based on the impacts resulting from sharing concocted content. Lastly, some have opted

for a hybrid approach.[6] The Czech Republic privileges the content-related approach. Section 16 of the Electoral Code states, "The election campaign must be honest and fair. No false information on individual candidates and political parties or coalitions, on whose candidate lists the candidates are featured, may be published"(Czech Parliament 1995:16). A total of 12 United States electoral laws also contain provisions against electoral procedural disinformation, such as California, New York, and Pennsylvania (Movement Advencement Project (MAP) 2024). The Canada Elections Act makes it illegal to distribute false information about candidates' "citizenship, place of birth, education, professional qualifications or membership in a group or association"[7] (Government of Canada 2000:91). Article 57 of the Election Code of Ukraine (as amended in July 2020) makes it illegal "to spread deliberately false information about the candidate or party (party organization) that are electoral subjects" (Republic of Ukraine 2020:57). This legislative approach has limited effectiveness, as it only protects a narrow range of information typically not targeted by disinformation campaigns.

Other EMBs privilege the consequentialist approach. Article 132 of the Electoral Code of Mali stipulates that

> "[t]hose who, using false news, slander or other fraudulent maneuvers, have diverted votes or have determined one or more voters to abstain from voting, will be punished by imprisonment of one (01) month to one (01) year and a fine of twenty-five thousand (25,000) to two hundred fifty-thousand (250,000) francs." (République du Mali n.d.:132) (free translation).

In Austria, the Criminal Code provides that

> "[a]ny person who publicly disseminates false information about a circumstance that is likely to deter persons entitled to vote or to vote from voting or to induce them to exercise their right to vote in a particular way at a time when a counterstatement can no longer be effectively disseminated shall be liable to a custodial sentence not exceeding six months or to a monetary penalty of up to 360 daily penalty units." (Article 264).

The Brazilian Congress introduced in 2020 the pending Bill of Law on Freedom, Responsibility and Transparency on the Internet, which would make it illegal to disseminate false information to attack the credibility of elections (José Guimarães - PT/CE 2024; Vieira 2020). In 2023, the defence minister of Taiwan proposed to amend the All-out Defense Mobilization Readiness Act to

6 ADTAC Disinventory provides a good overview of countries' policies to fight disinformation. See https://inventory.adt.ac/wiki/National_Policies_Affecting_Disinformation.

7 Even then, courts have rarely convicted people for such a crime as it is tough to prove that someone intentionally shared information they knew to be counterfactual (Gaumond 2020). Sharing false information is, therefore, not a crime unless it can be proven that it was done with full knowledge of the facts and with the willful intention of distorting the conditions of the vote

include measures that are aimed at combating "cognitive warfare," which refers to the dissemination of disinformation or rumours that pose a threat to society and the general public (Chan 2023). This bill has not been officially approved due to uncertainties surrounding specific provisions and their implementation (Souza, 2023). With an even more forceful approach, the French parliament adopted in 2018 the "Law Against the Manipulation of Information" (*Loi contre la manipulation de l'information*), which aims to combat the various forms of intentional dissemination of fake news. During the three months preceding a national election, a judge can use this law to rapidly halt the circulation of a publication by the following three criteria: i) the false news must be evident; ii) be disseminated on a massive scale and artificially; and iii) lead to a *disturbance of the public peace* or the *sincerity of an election* (République française 2018)[8].

Latvian authorities have taken a hybrid approach. The Criminal Law considers an offence the act of hooliganism, which is to carry out "a gross disturbance of the public order, which is manifested in obvious disrespect for the public or in insolence, ignoring generally accepted standards of behaviour and disturbing the peace of persons or the work of institutions" (Tieslietu ministrija 2022)[9]. Although spreading disinformation could rightly be considered an act of hooliganism, some are calling for this law to be overhauled so that it can be used more specifically to deal with disinformation, given the extent of this phenomenon today (Zāģere and Treļs 2022). Besides this legislation, Latvia adopted a different legislative path that should have an impact on disinformation, as the Parliament approved in September 2023 the 'National Security Concept,' a government-backed policy planning document. It states that as of 1 January 2026, all content created by public media must only be in Latvian and languages belonging to the European cultural space (Eng.LSM.lv 2023). The move will prohibit Latvian media from producing content in Russian. As most disinformation efforts in Latvia target the Russian-speaking minority, this legislation will presumedly contribute to curbing disinformation[10].

Have any of the three legal initiatives been effective in combating electoral disinformation? It is premature to give a definitive answer, as evaluating the impact of such legislation is complex, given that disinformation is a relatively new phenomenon and long-term data is limited. Most studies of laws designed to limit the spread of false or misleading information on social media focus on the consequences of freedom of expression, rather than on their

8 This law has been used only once, and the complainants were unsuccessful because, according to the judges who examined the complaint, the shared information was not covered by the law.

9 For a good overview of EU legislations that limit the spread of disinformation, false news and fake news, see (Hoboken and Fathaigh 2021).

10 Some nations have enacted regulations in response to the issue of disinformation, although most of these laws predate the widespread use of technology and social media. For instance, Croatia's Electronic Media Act forbids discrimination based on factors such as race, gender, or religion. It also contains bans on apologizing for fascism or communism. (Hrvatski sabor (*The Parliament of Croatia*) 2009).

effectiveness[11]. Additionally, other factors beyond the reach of these laws may have contributed to any observed different pattern of behaviour in disinformation campaigns. Studies have shown trends in Russian disinformation campaign operations that are primarily linked to geopolitical objectives that the Kremlin wishes to reach. For instance, since 2020, Russia has intensified its engagement in the Sahel region with the objective of reshaping the region's strategic landscape and undermining Western influence (Terren, Aelst, and Damme 2025). We should therefore be cautious to accredit the reduction of disinformation solely on the effectiveness of laws.

Foreign interference cases are even more straightforward. As stated above, EMBs do not exercise national security or defence powers, which is entirely legitimate. Crucially more critical, however, they do not have any authority beyond their territory, even in areas where they are competent. Even if they could identify malign actors behind foreign electoral manipulative operations and convince legal authorities to initiate criminal proceedings against individuals or entities that violated electoral laws, these proceedings would be ineffective if the alleged offenders resided outside the country[12]. This is because extradition agreements between like-minded states are rare. Such a treaty does not bind Russia, China and Iran. Incidentally, identifying adverse online authors is also challenging, insomuch as widely available tools such as Virtual Private Networks (VPNs) allow users to maintain online anonymity easily. (Desai, Pawelec, and Lesher, 2022).

EMB's Range of Actions is Limited by Strict Independence and Impartiality

The third limitation EMBs face in their fight against new electoral risks is their severe restriction due to the obligation of independence and impartiality. This constraint obliges them to show strict neutrality to ensure equality of opportunity between candidates. For instance, Austrian Returning Officers "have to make a vow as to their impartiality and conscientious fulfilment of their duties to the person who appointed them" (Bunderskamzlermat Österreich 1992:2)[13].

11 See for instance (Lim and Bradshaw 2023).

12 The remark made by David Vigneault, the director of the Canadian Security Intelligence Services, during the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions well summarizes this difficulty: "Ultimately, state actors [were] able to conduct [foreign interference] successfully in Canada because there are no consequences, either legal or political. [Foreign interference] is therefore a low-risk and high-risk endeavour." (Vigneault 2024).

13 Somewhat surprisingly, the majority of electoral laws, which define the composition of the members of EMBs, their duties and responsibilities, do not specify that they must act in a neutral, objective and non-partisan manner. In some cases, as in Singapore, they only have to confirm that they are not a political party member on the day of the vote, which seems to me to be a very weak constraint and guarantee of integrity. This issue would certainly merit further analysis. Cf. The Statute of the Republic of Singapore. Presidential Elections Act (Chapter 240A), 2011, Part II, Elections (ELD n.d.). In the case of Luxembourg, the legislator has prohibited election staff from being affiliated or related to candidates and elected persons, but nothing is mentioned about their

In Canada, any election officer must make a solemn declaration before assuming duties that "he or she will exercise the powers and perform the duties of the office in an impartial manner" (Ministère de la Justice 2023:3).[14] To ensure non-partisanship, members of Guatemala's Supreme Electoral Tribunal (*Tribunal Supremo Electoral*) cannot be a member of any political party (Asamblea Nacional Constituyente 2017:124).

This neutrality requirement severely limits any role EMBs may perform in defence of a candidate that is the subject of a partisan disinformation campaign, as this may be interpreted as one-sidedness. Even where EMBs wield greater leverage, such as the Costa Rican Supreme Electoral Tribunal (TSE), its actions must be strictly limited and concordant with its constitutional obligation, and for this reason, its members are forbidden to "enter into debate with candidates or competing parties" (Gustavo 2023:56). TSE must be left to journalists and fact-checkers to debunk partisan disinformation. The nature of EMBs is that they must remain neutral. This prevents them from acting against disinformation and foreign interference, especially when partisan elements are involved, which is often the case. To overcome this limitation, EMBs should focus on addressing procedural disinformation, as this type of threat can be handled in an objective and fair way.

Social Media Platform Cannot Regulate Their Content, and This Includes Disinformation.

The fourth and final limitation faced by EMBs in addressing new electoral risks presents a dual constraint. Similar to the first limitation, EMBs lack authority over the legislative framework necessary to enact legal reforms that would enhance resilience to these threats. Specifically, they cannot impose regulatory measures on social media platforms to ensure more stringent oversight of election-related content, despite these platforms playing a crucial role in the dissemination of disinformation. Furthermore, even if EMBs were to succeed in advocating for such reforms, the permissive terms of use and limited liability provisions governing these platforms enable them to disregard a substantial volume of online content and its creators. They simply ignore most of what circulates on their platforms.

This issue is compounded by the fact that a very important portion of social media platform traffic comprises inauthentic pages produced by automated bots (Binder 2024; Bischoff 2021; Kargl 2023). A report written in 2019 by

membership of political parties or their duty of neutrality and objectivity. See Loi électorale du 18 février 2003, Chapitre II. De la composition des bureaux, article 67. Cf. https://elections.public.lu/dam-assets/fr/legislation/loi-electorale-18-02-2003.pdf

14 This requirement for neutrality and non-partisanship is applied in various ways, considering the different organizational models of EMBs, particularly in cases where EMB members are representatives of political parties, as in Colombia, for example. In such cases, requiring them to put partisanship aside would be in conflict with the very principle behind the law.

former Facebook data scientist Jeff Allan well illustrates this phenomenon. In the United States, "6 of the top 10 pages visited by the African-American community were pages produced by troll farms" based in Kosovo and Macedonia (Allen 2019). The authors of these sites were not from this community, nor were they even designed to bring community members together to share their views and promote their interests. Their creators exploited Facebook's advertising revenue model, which favours popular content (Alexander 2016). And yet, despite the inauthentic nature of these pages and the fact that this phenomenon is documented, the platform has done little to restrict their distribution. Although platforms occasionally say that they have removed hacked accounts and adopted tools to identify inauthentic online behaviours, in reality, because this phenomenon is so vast, the scale of such efforts is insufficient to have an impact (Nimmo 2022; Safi 2019; Sawers 2022; Timberg and Dwoskin 2019). It is likely to grow, as counterfeiters now have the tools to deepfake digital content using artificial intelligence, making their task even easier (Mai et al. 2023).

If it is difficult for platforms to measure the phenomenon of online inauthenticity, it is even more difficult for third parties, such as legislators, to recommend solutions to counter disinformation, as they also have very little access to the massive data that these platforms accumulate and that would enable a better understanding of this phenomenon. As private companies, they are reluctant to share such data (Persily and Tucker 2021). Social scientists and journalists complain about the lack of collaboration and transparency in social media so that they can better understand, among other things, how the algorithms and assumptions that power social media platforms work (Krass 2022; Mayer-Schönberger and Ramge 2022). Sometimes, the relationship between researchers and platforms is even more problematic. In 2021, for example, Meta forced the AlgorithmWatch research group to stop using an add-on script it had developed, which volunteer users could add to their profiles to understand better Instagram's News Feed algorithm (Kayser-Bril 2021). The issue of data access has also grown after platform X adopted in 2023 a new, more restrictive policy explicitly aimed at the research community (Jingnan, 2023). Lastly, the social media environment is ever-developing, and platform changes might contribute to disinformation. In a recent analysis, Reporters Without Borders condemned X since Elon Musk took it over in October 2022 to have become a "sanctuary for disinformation" (Berthier 2023). One cannot reliably predict future trends in the spread of online disinformation, but the lack of cooperation from social media platforms with authorities poses a real challenge for EMBs, as for any other actors in addressing new electoral risks.

What could EMBs do?

Election administrators worldwide recognize the danger that new electoral risks pose to the integrity of elections. Positioned at the forefront of electoral processes, they are well-placed to assess the scope and impact of these challenges. However, effectively addressing such risks remains a complex and

difficult task. Despite their limited powers, EMBs retain the capacity to implement measures aimed at mitigating these threats and safeguarding the integrity of electoral systems. One potential avenue is leveraging their legislative authority to regulate partisan and third-party advertising, as some have already done. However, they must set realistic expectations with this strategy, as the effectiveness of such regulations in mitigating the spread of disinformation is likely to be minimal, given that social media advertising is not the primary vehicle for disseminating false information (Dawsey 2017). The disinformation ecosystem is complex and widespread, operating through networks that extend beyond paid advertisements. While there have been instances of disinformation disseminated through social media advertising, they are infrequent (Marks 2021:388). Access to this space is restricted not only because it is a paid service, but also because it is already subject to a series of regulatory provisions limiting its misuse. For these reasons, disinformation takes many other paths, such as on Facebook group pages (Alexander and Silverman 2016), in private messages on WhatsApp (Hern 2020), on Snapchat (Andrey et al. 2021), on X (Singh and Blase 2020; Vosoughi, Roy, and Aral 2018). During the 2018 Brazilian presidential election, X was one of the prominent supporters of disinformation (Recuero 2020). During the 2019 Tunisian presidential elections, disinformation proliferated mainly through Facebook posts (Jouini 2019). During the 2019 Indian general elections, WhatsApp users were the main target of disinformation by other users of the platforms (Garimella and Eckles, 2020). During the 2018 Mexican presidential elections, numerous fake opinion polls were published on social media and on some traditional media (Buendia 2018). These examples testify to the wide variety of spaces available to spread disinformation outside advertising. Consequently, while regulatory frameworks on political advertising may contribute to greater transparency, their overall impact on curbing disinformation remains constrained.

From an administrative standpoint, and beyond the limitations of this inconclusive legislative approach, EMBs should adopt a more comprehensive risk management framework in the planning and execution of elections, as recommended by researchers from International IDEA in 2021 (Vincent, Alihodzic, and Gale 2021). A preliminary review of the publicly available strategic plans of various EMBs suggests that this approach has not yet been widely adopted. Given that disinformation and foreign interference operations often occur outside official electoral campaigns, they should actively support initiatives aimed at establishing a whole-of-government approach to address these challenges[15]. EMBs alone do not have the necessary resources to mitigate this threat, nor is it in their mandate.

15 As recommended by O'Connor, Sarah, Fergus Hanson, Emilia Currey, and Tracy Beattie (2020), "Cyber-enabled foreign interference in elections and referendums," *International Cyber Policy Centre at ASPI* 63; and Hogue, Marie-Josée (2024), "Initial Report," Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions, 194.

Given that most EMBs are mandated to educate voters, they should mount campaigns focused on identifying disinformation, enhancing media literacy, and promoting fact-checking, with a particular emphasis on countering procedural disinformation. Recognizing the significant role that political parties and candidates play in the electoral process, EMBs should also develop specialized educational toolkits and training programs tailored to these stakeholders. By equipping them with the necessary knowledge and resources, EMBs can foster a more resilient electoral environment. However, despite the value of these initiatives, here again it is essential that they establish realistic expectations regarding the effectiveness of these measures in combating disinformation. In their study on the effectiveness of fact-checking, Nathan Walter and his colleagues showed that preexisting ideological beliefs reduce the ability to identify factual information. And yet, this is particularly this segment of the population who would benefit the most from such efforts (Walter et al. 2020). Moreover, if we consider disinformation a public health issue, as it can harm society by altering voters' choices, studies have shown that simply correcting the record may not effectively reduce the risk-taking behaviour of less cognitively capable voters, as they have more difficulty distinguishing between information and disinformation[16]. (Adams et al. 2023; De keersmaecker and Roets 2017; Yadav and Kobayashi 2015).

To enhance the robustness of the EMB's communication link with voters and contenders, we suggest that they avoid using social media for disseminating election-related content and instead rely solely on their official websites, where they maintain full authority over the messaging. As a last remark, while it is key to offer convenient voting methods to reduce the cost of voting and increase voter turnout, EMBs should continue to use paper ballots alongside these measures. The risk of significant electoral manipulation, whether foreign or not, is much greater with online systems than with paper ballots and human-administered processes.

16 This is the conclusion that Rajendra-Prasad Yadav and Miwako Kobayashi reached in their study of mass media campaigns for reducing alcohol-impaired driving and alcohol-related crashes. They found that "[d]espite additional decades of evidence, reviewed studies were heterogeneous in their approaches; therefore, we could not conclude that media campaigns reduced the risk of alcohol-related injuries or crashes." Yadav, Rajendra-Prasad, and Miwako Kobayashi (2015), "A systematic review: effectiveness of mass media campaigns for reducing alcohol-impaired driving and alcohol-related crashes," *BMC Public Health* 15: 857. Similarly, Zoë Adams, Magda Osman et al. Have found that "in health and risk communication it is widely accepted that the mere provision of accurate information is typically not sufficient to induce behavioral change—raising the question of why perceiving false information should be sufficient to induce aberrant behaviour." Adams, Zoë, Magda Osman, Christos Bechlivanidis, and Björn Meder (2023), "(Why) Is Misinformation a Problem?", *Perspectives on Psychological Science* 18(6): 143663.

Conclusion

The dissemination of knowingly false information and the manipulation of electoral processes by foreign entities are a rising concern that poses a threat to the integrity of democratic elections. Both phenomena compromise the integrity of electoral processes and alter the attitudes and behaviours of electors in a manner that is counter to a healthy democracy. While EMBs are cognizant of the gravity of this threat, their capacity to safeguard elections is constrained by their limited legal autonomy and the absence of straightforward solutions to address these challenges. A confluence of factors, intrinsic to both the capacities of EMBs and the nature of the threat, imposes considerable constraints on their ability to effectively intervene. First, EMBs are unable to amend electoral legislation, a necessary step to combat this threat, due to their inability to exercise legislative autonomy. Instead, EMBs rely on parliamentarians for any amendments to electoral legislation and, for partisan reasons, they infrequently act. Second, the challenge of protecting against disinformation is compounded by the fact that it most often classifies as free speech, which hinders the imposition of sanctions. Furthermore, foreign entities engaging in malign activities during electoral processes are not subject to national legal jurisdiction. Third, any measures that EMBs might take against partisan disinformation would be inconsistent with their obligations of neutrality. The fourth and final constraint, while compelling social media platforms to enhance content curation, would be helpful, as they host most of the disinformation, EMBs do not possess such authority and social media platforms can hardly enforce any regulation over what circulates online.

Acknowledgements:

I would like to thank the reviewers for their constructive and insightful comments.

References

Adams, Zoë et al. 2023. “(Why) Is Misinformation a Problem?” *Perspectives on Psychological Science* 18 (6): 1436–1463. doi: 10.1177/17456916221141344.

ADF. 2023. “On a découvert un « vaste réseau » de plateformes russes de désinformation qui cible l’Afrique.” *Africa Defense Forum*.

Ahmetaj, Burim. 2021. “Interview with Burim Ahmetaj, Chief Executive Officer at Central Election Commission of Kosovo.”

Alexander, Lawrence, and Craig Silverman. 2016. “How Teens In The Balkans Are Duping Trump Supporters With Fake News.” *BuzzFeed News*. https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo (last accessed : April 18, 2024).

_____. 2016. “How Macedonian Spammers Are Using Facebook Groups To Feed You Fake News.” *BuzzFeed News*. https://www.buzzfeednews.com/article/craigsilverman/how-macedonian-spammers-are-using-facebook-groups-to-feed-yo (last accessed : July 29, 2022).

Allen, Jeff. 2019. *How Communities Are Exploited on Our Platforms: A Final Look at the "Troll Farms" Pages*.
Andrey, Sam et al. 2021. *Private Messaging Public Harms: Disinformation and Online Harms on Private Messaging Platforms in Canada*. Ryerson Leadership Lab.
Asamblea Nacional Constituyente. 2017. *Ley Electoral y de Partidos Políticos*.
Australian Electoral Commission. 2018. "Electoral Integrity Assurance Taskforce." *Australian Electoral Commission*. https://www.aec.gov.au/elections/electoral-advertising/electoral-integrity.html (last accessed : January 11, 2022).
_____. 2023a. *2023 Corporate Plan*. AEC.
_____. 2023b. "Disinformation Register." *Australian Electoral Commission*. https://www.aec.gov.au/media/disinformation-register.htm (last accessed : January 9, 2024).
Benoit, Kenneth. 2004. "Models of Electoral System Change." *Electoral Studies* 23 (3): 363–389. doi: 10.1016/S0261-3794(03)00020-9.
Berthier, Vincent. 2023. "From Twitter to X, Elon Musk's Transformation from Free Speech Defender to Champion of Disinformation | RSF." https://rsf.org/en/twitter-x-elon-musk-s-transformation-free-speech-defender-champion-disinformation (last accessed : December 5, 2023).
Binder, Matt. 2024. "The Majority of Traffic from Elon Musk's X May Have Been Fake during the Super Bowl, Report Suggests." *Mashable*. https://mashable.com/article/x-twitter-elon-musk-bots-fake-traffic (last accessed : May 28, 2024).
Bischoff, Paul. 2021. "Inside a Facebook Bot Farm That Pumps out 200k+ Political Posts per Month." *Comparitech*. https://www.comparitech.com/blog/information-security/inside-facebook-bot-farm/ (last accessed : May 28, 2024).
Boegman, Anton. 2020. *Digital Communications, Disinformation and Democracy: Recommendations for Legislative Change*. Elections BC.
Boston Globe. 2022. "Election Workers Are under Assault. We Need to Protect Them. Now.: The Crisis Roiling the Profession Is a Crisis of Democracy." *Boston Globe*, November 8, A.8.
Boulay, Sophie. 2015. *Usurpation de l'identité citoyenne dans l'espace public. Astroturfing, communication et démocratie*. Québec: Presses de l'Université du Québec.
Brown, Étienne. 2021. "Opinion | Facebook Is Creating a New Digital Divide — One That Separates Anglophones from Users Who Do Not Speak English." *The Toronto Star*, November 19.
Buendia, Jorge. 2018. *Fake Polls as Fake News: The Challenge for Mexico's Elections*. Wilson Center. Mexico Institute.
Bunderskamzlermat Österreich. 1992. *Bundesgesetz Über Die Wahl Des Nationalrates*.
Business News. 2019. "Salma Elloumi ne s'est pas désistée en faveur de Abdelkarim Zbidi." *www.businessnews.com.tn*. https://www.businessnews.com.tn/Selma+Elloumi+ne+s%92est+pas+d%E9sist%E9e+en+faveur+de+Abdelkarim+Zbidi%0D%0A%0D%0A,540,90850,3 (last accessed : August 16, 2023).
Censky, Abigail. 2021. "How Misinformation Lit The Fire Under A Year Of Political Chaos In Michigan." *NPR*, January 1.
Chan, Minnie. 2023. "Taiwan's Plans to Target Fake News Fan Fears of Threat to Press Freedom." *South China Morning Post*. https://www.scmp.com/news/china/military/article/3211732/taiwans-plans-target-fake-news-fan-fears-threat-press-freedom (last accessed : December 5, 2023).
Clucas, Tom. 2020. "'Don't Feed the Trolls.'" In: Sara Polak, and Daniel Trottier, eds. *Violence and Trolling on Social Media: History, Affect, and Effects of Online Vitriol*. Amsterdam: Amsterdam University Press: pp.: 47–64.

Crain, Matthew, and Anthony Nadler. 2019. "Political Manipulation and Internet Advertising Infrastructure." *Journal of Information Policy* 9: 370–410. doi: 10.5325/jinfopoli.9.2019.0370.
Czech Parliament. 1995. *Czech Law on Parliamentary Elections*.
Dave, Aashka, Emily Boardman Ndulue, and Laura Schwartz-Henderson. 2020. *Targeting Greta Thunberg: A Case Study in Online Mis/Disinformation*. German Marshall Fund of the United States.
Dawsey, Josh. 2017. "Russian-Funded Facebook Ads Backed Stein, Sanders and Trump." *Politico*. https://www.politico.com/story/2017/09/26/facebook-russia-trump-sanders-stein-243172 (last accessed : August 14, 2023).
De keersmaecker, Jonas, and Arne Roets. 2017. "'Fake News': Incorrect, but Hard to Correct. The Role of Cognitive Ability on the Impact of False Information on Social Impressions." *Intelligence* 65: 107–110. doi: 10.1016/j.intell.2017.10.005.
Democratic Institutions. 2020. "Report on the Assessment of the Critical Election Incident Public Protocol." https://www.canada.ca/en/democratic-institutions/services/reports/report-assessment-critical-election-incident-public-protocol.html (last accessed : May 21, 2024).
Department of Home Affairs. 2024. "Department of Home Affairs Website." *Department of Home Affairs Website*. https://www.homeaffairs.gov.au (last accessed : January 30, 2025).
Desai, Arpitha, Hanna Pawelec, and Molly Lesher. 2022. *Disentangling Untruths Online: Creators, Spreaders and How to Stop Them*. *Going Digital Toolkit Notes*. 23. OECD Publishing. doi: 10.1787/84b62df1-en.
Die Bundeswahlleiterin. 2021. "Facts against Fake News - The Federal Returning Officer." https://www.bundeswahlleiter.de/en/bundestagswahlen/2021/fakten-fakenews.html#b1f77833-c1f9-4167-9e83-51019b667552 (last accessed : August 31, 2021).
Die Bundeswahlleiterin. 2024. "Responsibilities - The Federal Returning Officer." *The Federal Returning Officer and Her Responsibilities*. https://www.bundeswahlleiterin.de/en/ueber-uns/aufgaben.html#b0d933c9-68d8-4893-9619-21b07065bf63 (last accessed : November 28, 2023).
ELD. n.d. "Elections Department Singapore." https://www.eld.gov.sg (last accessed : January 24, 2024).
Elections Alberta. 2023. *Strategic Plan 2024-2028*. Elections Alberta.
Elections BC. 2024. "Disinformation Register | Elections BC." https://elections.bc.ca/2024-provincial-election/election-integrity/disinformation-register/ (last accessed : January 24, 2024).
Elections Canada. 2024. "ElectoFacts." https://www.elections.ca/content.aspx?section=res&dir=dis&document=index&lang=e (last accessed : January 18, 2024).
Élections Québec. 2021. "S'informer pour faire un choix éclairé." *Élections Québec*. https://www.electionsquebec.qc.ca/comprendre/comprendre-le-vote/sinformer-pour-faire-un-choix-eclaire/ (last accessed : February 19, 2025).
_____. 2023. *Pour une nouvelle vision de la Loi électorale - Document de consultation*. Élections Québec.
_____. 2024. *Plans stratégiques 2024-2028*. Élections Québec.
Eng.LSM.lv. 2023. "Saeima Approves Updated National Security Concept for Latvia." (last accessed : April 10, 2024 (https://eng.lsm.lv/article/society/defense/28.09.2023-saeima-approves-updated-national-security-concept-for-latvia.a525735/).

Feertchak, Alexis. 2017. “Les Cinq «fake News» Qui Ont Pollué La Campagne Présidentielle.” *Le Figaro*. (https://www.lefigaro.fr/elections/presidentielles/2017/04/22/35003-20170422ARTFIG00048-les-cinq-fake-news-qui-ont-pollue-la-campagne-presidentielle.php (last accessed : March 10, 2025).

Garimella, Kiran, and Dean Eckles. 2020. “Images and Misinformation in Political Groups: Evidence from WhatsApp in India.” *Harvard Kennedy School Misinformation Review*. doi: 10.37016/mr-2020-030.

Garnett, Holly Ann, and Michael Pal, eds. 2022. *Cyber-Threats to Canadian Democracy*. McGill-Queen’s University Press.

Gaumond, Eve. 2020. “Is Canadian Law Better Equipped to Handle Disinformation?” *Lawfare*. https://www.lawfareblog.com/canadian-law-better-equipped-handle-disinformation (last accessed : January 31, 2022).

Gessen, Masha. 2018. “Why the Russian Influence Campaign Remains So Hard to Understand.” *The New Yorker*, December 18.

Gethin, Amory, Clara Martínez-Toledano, and Thomas Piketty. 2021. “Brahmin Left Versus Merchant Right: Changing Political Cleavages in 21 Western Democracies, 1948–2020.” *The Quarterly Journal of Economics* 137 (1): 1–48. doi: 10.1093/qje/qjab036.

Gill, Lex. 2020. *Les aspects juridiques du discours haineux au Canada*. Expression démocratique.

Government of Canada. 1986. *Competition Act (R.S.C., 1985, c. C-34)*.

_____. 2000. *Canada Elections Act (S.C. 2000, c. 9)*.

Gustavo, Román Jacobo. 2023. «Los organismos electorales frente a la desinformación. Memoria y lecciones aprendidas por el TSE tras las elecciones nacionales de 2022.” *Revista de Derecho Electoral* (35): 29–58. doi: 10.35242/RDE_2023_35_3.

Helmus, Todd C. 2022. *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*. RAND Corporation.

Hern, Alex. 2020. “WhatsApp to Impose New Limit on Forwarding to Fight Fake News.” *The Guardian*, April 7.

Hoboken, Joris van, and Ronan Ó. Fathaigh. 2021. “Regulating Disinformation in Europe: Implications for Speech and Privacy.” *UC Irvine Journal of International, Transnational, and Comparative Law* 6 (1): 9.

Hogue, Marie-Josée. 2024. *Initial Report*. Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions.

Hrvatski sabor. 2009. *Zakon o Elektroničkim Medijima*.

INE. 2017. “Instituto Nacional Electoral.” https://portalanterior.ine.mx/archivos3/portal/historico/contenido/Que_es/ (last accessed : February 28, 2025).

Irish, John. 2023. “France Says It Uncovered Mass Russian-Linked Misinformation Campaign.” *Reuters*, June 13.

Jacobs, Kristof, and Monique Leyenaar. 2011. “A Conceptual Framework for Major, Minor, and Technical Electoral Reform.” *West European Politics* 34 (3): 495–513. doi: 10.1080/01402382.2011.555977.

Jalli, Nuurrianti. 2023. “TikTok’s Poor Content Moderation Fuels the Spread of Hate Speech and Misinformation Ahead of Indonesia 2024 Elections.” *The Conversation*. http://theconversation.com/tiktoks-poor-content-moderation-fuels-the-spread-of-hate-speech-and-misinformation-ahead-of-indonesia-2024-elections-202439 (last accessed : November 28, 2023).

Jeangène Vilmer, J. B. et al. 2018. *Les manipulations de l’information : un défi pour nos démocraties*. Centre d’analyse, de prévision et de stratégie (CAPS) du ministère de l’Europe et des Affaires étrangères.

Jingnan, Huo. 2023. "Twitter's New Data Access Rules Will Make Social Media Research Harder." *NPR*, February 9.
José Guimarães - PT/CE. 2024. *Projeto de Lei 224/2024*.
Jouini, Yosr. 2019. "Ahead of Tunisia Elections, Social Media Was Flooded with Mis- and Disinformation." *Global Voices Advox*. https://advox.globalvoices.org/2019/10/22/ahead-of-tunisia-elections-social-media-was-flooded-with-mis-and-disinformation/ (last accessed : August 16, 2023).
Kargl, Denis. 2023. "TikTok's Massive Problem with Bots, Fake Accounts and Scam." *Fraud0*. https://www.fraud0.com/resources/tiktok-bots-fake-accounts-scam/ (last accessed : May 28, 2024).
Kayser-Bril, Nicolas. 2021. "AlgorithmWatch Forced to Shut down Instagram Monitoring Project after Threats from Facebook." *AlgorithmWatch*. https://algorithmwatch.org/en/instagram-research-shut-down-by-facebook/ (last accessed : September 2, 2021).
Kim, Jeong-Gon. 2024. "South Korea: An Independent and Neutral Electoral Management Body." *ACE. The Electoral Knowledge Network*.
Krass, Peter. 2022. "Transparency: The First Step to Fixing Social Media." *MIT Initiative on the Digital Economy*. https://ide.mit.edu/insights/transparency-the-first-step-to-fixing-social-media/ (last accessed : August 21, 2023).
Kusche, Isabel. 2019. "Pourquoi Le Micro-Ciblage Politique Pourrait Saper La Démocratie." *The Conversation*. http://theconversation.com/pourquoi-le-micro-ciblage-politique-pourrait-saper-la-democratie-116319 (last accessed : May 26, 2022).
Łabuz, Mateusz, and Christopher Nehring. 2024. "On the Way to Deep Fake Democracy? Deep Fakes in Election Campaigns in 2023." *European Political Science*. doi: 10.1057/s41304-024-00482-9.
Lajoie, Geneviève. 2022. "Les Québécois En Faveur d'une Réforme Du Mode de Scrutin." *Le Journal de Québec*, October 13.
Legislative Assembly of British Columbia. 2023. *Elections Amendment Act, 2023*.
Levi, Lili. 2022. "Disinformation and the Defamation Renaissance: A Misleading Promise of 'Truth.'" *University of Miami Legal Studies Research* (Paper No. 4254372).
Lim, Gabrielle, and Samantha Bradshaw. 2023. *Chilling Legislation: Tracking the Impact of "Fake News" Laws on Press Freedom Internationally*. The Center for International Media Assistance (CIMA).
Mai, Kimberly T. et al. 2023. "Warning: Humans Cannot Reliably Detect Speech Deepfakes." *PLOS ONE* 18 (8): e0285333. doi: 10.1371/journal.pone.0285333.
Marks, Jadyn. 2021. "Whose Lie Is It Anyway? Holding Social Media Sites Liable for Procedural Election Disinformation." *Federal Communications Law Journal* 74: 379.
Marshall, Hannah, and Alena Drieschova. 2018. "Post-Truth Politics in the UK's Brexit Referendum." *New Perspectives* 26 (3): 89–106.
Martin, Alexander. 2023. "Estonian Official Says Parliamentary Elections Were Targeted by Cyberattacks." *The Record*. https://therecord.media/estonia-cyberattack-parliamentary-elections (last accessed : January 26, 2024).
Mayer-Schönberger, Viktor, and Thomas Ramge. 2022. *Access Rules: Freeing Data from Big Tech for a Better Future*. Oakland, CA: University of California Press.
McBrien, Tyler. 2020. "Defending the Vote: Estonia Creates a Network to Combat Disinformation, 2016–2020." *Defending the Vote: Estonia Creates a Network to Combat Disinformation, 2016–2020*.
Ministère de la Justice. 2023. *Loi électorale du Canada (L.C. 2000, ch. 9)*.

Ministry of Justice of Jamaica. 2006. *The Electoral Commission (Interim) Act*.
Mohan, Vasu, and Alan Wall. 2019. "Foreign Electoral Interference: Past, Present, and Future." *Georgetown Journal of International Affairs* 20 (1): 110–116. doi: 10.1353/gia.2019.0019.
Movement Advencement Project (MAP). 2024. *Protections Against Election Disinformation*. Movement Advencement Project (MAP).
Nimmo, Ben. 2022. "Removing Coordinated Inauthentic Behavior From China and Russia." *Meta*. https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/ (last accessed : August 29, 2023).
Oficina Nacional de Procesos Electorales. 2022. "JNE y ONPE presentan asistentes virtuales en WhatsApp para brindar información sobre las elecciones regionales y municipales." https://www.gob.pe/institucion/onpe/noticias/648099-jne-y-onpe-presentan-asistentes-virtuales-en-whatsapp-para-brindar-informacion-sobre-las-elecciones-regionales-y-municipales (last accessed : January 9, 2024).
OICDE. 2022. "Observatorio Interamericano Para El Combate a La Desinformación Electoral | ONPE." *Observatorio Interamericano Para El Combate a La Desinformación Electoral | ONPE*. https://observatorio.onpe.gob.pe/ (last accessed : May 21, 2024).
ONPEChequea. 2022. "ONPEChequea." *Observatorio Interamericano Para El Combate a La Desinformación Electoral | ONPE*. https://observatorio.onpe.gob.pe/chequea/ (last accessed : January 9, 2024).
Osborn, Catherine. 2023. "Inside Latin America's Fake News Problem." *Foreign Policy*.
Pal, Michael. 2016. *Electoral Management Bodies as a Fourth Branch of Government. SSRN Scholarly Paper*. ID 2792626. Rochester, NY: Social Science Research Network.
Pariser, Eli. 2012. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. London: Penguin Books.
Persily, Nathaniel, and Joshua A. Tucker. 2021. "How to Fix Social Media? Start with Independent Research." *Brookings*. https://www.brookings.edu/articles/how-to-fix-social-media-start-with-independent-research/ (last accessed : August 21, 2023).
Qiu, Linda. 2021. "Fact-Checking Falsehoods on Mail-In Voting." *The New York Times*, January 5.
Recuero, Raquel. 2020. "#FraudenasUrnas: Estratégias Discursivas de Desinformação No Twitter Nas Eleições 2018: #FraudenasUrnas: Disinformation's Discursive Strategies on Twitter During Brazilian 2018 Elections." *Revista Brasileira de Lingüística Aplicada* 20(3):383–406. doi: 10.1590/1984-6398202014635.
Republic of Ukraine. 2020. *Election Code of Ukraine (as Amended July 2020)*.
République du Mali. n.d. *Loi N°2022-019 Du 24 Juin 2022 Portant Loi Électorale*.
République française. 2018. *LOI N° 2018-1202 Du 22 Décembre 2018 Relative à La Lutte Contre La Manipulation de l'information*.
Rosenbach, Eric, and Katherine Mansted. 2019. *The Geopolitics of Information*. Belfer Center for Science and International Affairs.
Safi, Michael. 2019. "WhatsApp 'deleting 2m Accounts a Month' to Stop Fake News." *The Guardian*, February 6.
Sawers, Paul. 2022. "TikTok Says Fake Account Removal Increased 61% to 33.6M in Q2 2022." *TechCrunch*. https://techcrunch.com/2022/09/28/tiktok-says-fake-account-removal-increased-61-to-33-6m-in-q2-2022/ (last accessed : August 29, 2023).

Schmitt, Michael. 2021. "Foreign Cyber Interference in Elections." *International Law Studies* 97 (1): 739–764.
Scottish Government. 2024. "New Hate Crime Laws Come into Force." https://www.gov.scot/news/new-hate-crime-laws-come-into-force/ (last accessed : May 10, 2024).
Seddon, Paul. 2023. "Cyber-Attack on UK's Electoral Registers Revealed." *Cyber-Attack on UK's Electoral Registers Revealed*, August 8.
Sessa, Maria Giovanna. 2022a. "Disinformation Self-Proclaimed Experts: Spreading COVID-19 Disinformation under the Guise of Expertise." *EU DisinfoLab*. https://www.disinfo.eu/publications/disinformation-self-proclaimed-experts-spreading-covid-19-disinformation-under-the-guise-of-expertise/ (last accessed : July 27, 2022).
_____. 2022b. "Ukraine Conflict Disinformation: Worldwide Narratives and Trends." *EU DisinfoLab*. https://www.disinfo.eu/publications/ukraine-conflict-disinformation-worldwide-narratives-and-trends/ (last accessed : July 27, 2022).
Sharpe, Robert J. 1987. "Commercial Expression and the Charter." *The University of Toronto Law Journal* 37 (3): 229–259. doi: 10.2307/825746.
Singh, Spandana, and Margerite Blase. 2020. *Google. Protecting the Vote.* New America.
South African Government. 1996. *Electoral Commission Act 51 of 1996*.
Souza, Moises de. 2023. "Controversy and Concerns: Taiwan's All-Out Defense Mobilization Act Bill Under Debate." *Modern Diplomacy*. https://moderndiplomacy.eu/2023/04/07/controversy-and-concerns-taiwans-all-out-defense-mobilization-act-bill-under-debate/ (last accessed : December 20, 2023).
Supreme Court of Canada. 2013. *Saskatchewan (Human Rights Commission) c. Whatcott*. Vol. 1.
Taboada, Carolina. et al. 2023. *Dealing with Disinformation in the 2022 Elections*. Igarape Institute.
Tenove, Chris et al. 2018. "Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy." *SSRN Electronic Journal*. doi: 10.2139/ssrn.3235819.
Terren, Ludovic, Peter Van Aelst, and Thomas Van Damme. 2025. *Shifting Alliances in West Africa: Measuring Russian Engagement to Support Counter-FIMI Strategies*. European Institute for Security Studies.
The Electoral Commission. 2023. "Reforming Electoral Law | Electoral Commission." *Reforming Electoral Law*. https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-priorities-reforming-elections/reforming-electoral-law (last accessed : November 28, 2023).
The Electoral Commission. 2024. "Electoral Integrity." *Electoral Commission*. https://www.electoralcommission.ie/what-we-do/electoral-integrity/ (last accessed : January 25, 2024).
Thompson, Nicole. 2022. "Three of Ontario's Four Main Parties Say They Favour Electoral Reform | CBC News." *CBC*. https://www.cbc.ca/news/canada/toronto/elxn-ont-electoral-reform-1.6462901 (last accessed : August 8, 2023).
Tieslietu ministrija. 2022. "Ministry of Justice of The Republic of Latvia's Clarification of the Amendments to Criminal Law Concerning Deliberate Dissemination of False Information Both in the Public Sphere and in the Digital Environment." https://www.tm.gov.lv/en/article/ministry-justice-republic-latvias-clarification-amendments-criminal-law-concerning-deliberate-dissemination-false-information-both-public-sphere-and-digital-environment (last accessed : December 5, 2023).

Timberg, Craig, and Elizabeth Dwoskin. 2019. “Twitter Is Sweeping out Fake Accounts like Never before, Putting User Growth at Risk.” *Washington Post*, December 23.
Tribunal Superior Eleitoral. 2022. “Sistema de alertas.” *Justiça Eleitoral*. https://www.tse.jus.br/eleicoes/sistema-de-alertas (last accessed : February 12, 2025).
Union européenne. 2022. “L’UE impose des sanctions aux médias publics RT/Russia Today et Sputnik, qui diffusent dans l’UE.” https://www.consilium.europa.eu/fr/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/ (last accessed : May 10, 2022).
US Justice Department. 2024. “Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere | United States Department of Justice.” https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence (last accessed : January 30, 2025).
Vallée, Pierre. 2023. *Droit électoral québécois Repères et enjeux contemporains*. Wilson & Lafleur.
Vie publique. 2021. “Loi organique 29 mars 2021 mesures élection Président de la République.” *vie-publique.fr*. http://www.vie-publique.fr/loi/277851-loi-organique-29-mars-2021-mesures-election-president-de-la-republique (last accessed : November 28, 2023).
Vieira, Senador Alessandro. 2020. *PL 2630/2020 - Senado Federal*.
Vigneault, David, dir. 2024. *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions. Public Hearing of 12 April 2024*.
Vilmer, Jean-Baptiste Jeangène. 2019. *The “Macron Leaks” Operation: A Post-Mortem*. The Atlantic Council.
Vincent, Amy, Sead Alihodzic, and Stephen Gale. 2021. *Risk Management in Elections: A Guide for Electoral Management Bodies*. Australian Electoral Commission and the International Institute for Democracy and Electoral Assistance.
Vosoughi, Soroush, Deb Roy, and Sinan Aral. 2018. “The Spread of True and False News Online.” *Science* 359 (6380): 1146–1151. doi: 10.1126/science.aap9559.
Walker, Julian. 2018. “Discours haineux et liberté d’expression : balises légales au Canada.” 30.
Walter, Nathan et al. 2020. “Fact-Checking: A Meta-Analysis of What Works and for Whom.” *Political Communication* 37 (3): 350–375. doi: 10.1080/10584609.2019.1668894.
Wardle, Claire, and Hossein Derakhshan. 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe.
Yadav, Rajendra-Prasad, and Miwako Kobayashi. 2015. “A Systematic Review: Effectiveness of Mass Media Campaigns for Reducing Alcohol-Impaired Driving and Alcohol-Related Crashes.” *BMC Public Health* 15:857. doi: 10.1186/s12889-015-2088-4.
Zāģere, Gunda, and Ēriks Treļs. 2022. “Viltus ziņu izplatīšanas krimināltiesiskais raksturojums.”
Zimonjic, Peter. 2024. “Foreign Interference Cost Conservative Party up to 9 Seats in 2021, O’Toole Tells Inquiry.” *CBC News*, April 3.

Ijan Parento

Prevazilaženje ograničenja: Izborna tela i borba protiv dezinformacija i stranog uticaja

Apstrakt:

Problem dezinformacija i stranog mešanja u izbore značajno je porastao u poslednjim godinama. Time se stvaraju neravnopravni uslovi koji ometaju fer konkurenciju i informisano glasanje. Izborne dezinformacije ispoljavaju se na dva načina: partijski i proceduralni. Partijske dezinformacije ciljaju na kandidate i birače lažnim informacijama kako bi uticali na njihove biračke preferencije. Proceduralne dezinformacije, s druge strane, imaju za cilj da obesprave birače ili da dovedu u pitanje izborni proces. Strano mešanje u izbore može se definisati kao svaki pokušaj uticaja na ishod izbora u drugoj zemlji. Da li su tela za upravljanje izborima (EMBs) sprovela efikasne mere za ublažavanje ovih rizika? Odgovor je složen, ali je u suštini – ne. Ona se suočavaju sa institucionalnim, pravnim i tehničkim ograničenjima koja im sputavaju delovanje. Prvo, izborna tela ne mogu menjati izborne zakone kako bi ih učinila otpornijim na pretnje dezinformacijama i stranog mešanja u izbore. Drugo, dezinformacije u većini slučajeva nisu krivično delo i ne potpadaju pod važeće zakone, što otežava pravno gonjenje. Strano mešanje izlazi izvan domašaja nacionalne jurisdikcije. Treće, postupci koje izborna tela mogu preduzeti ograničeni su njihovom obavezom da ostanu pravična i nepristrasna. Četvrto, iako bi unapređenje kontrole sadržaja na društvenim mrežama bilo korisno, izborna tela nemaju ovlašćenja da sprovedu takve mere, dok same platforme imaju ograničenu kontrolu nad objavljenim sadržajem.

Ključne reči: Izborna tela, dezinformacije, strano mešanje u izbore, izbori