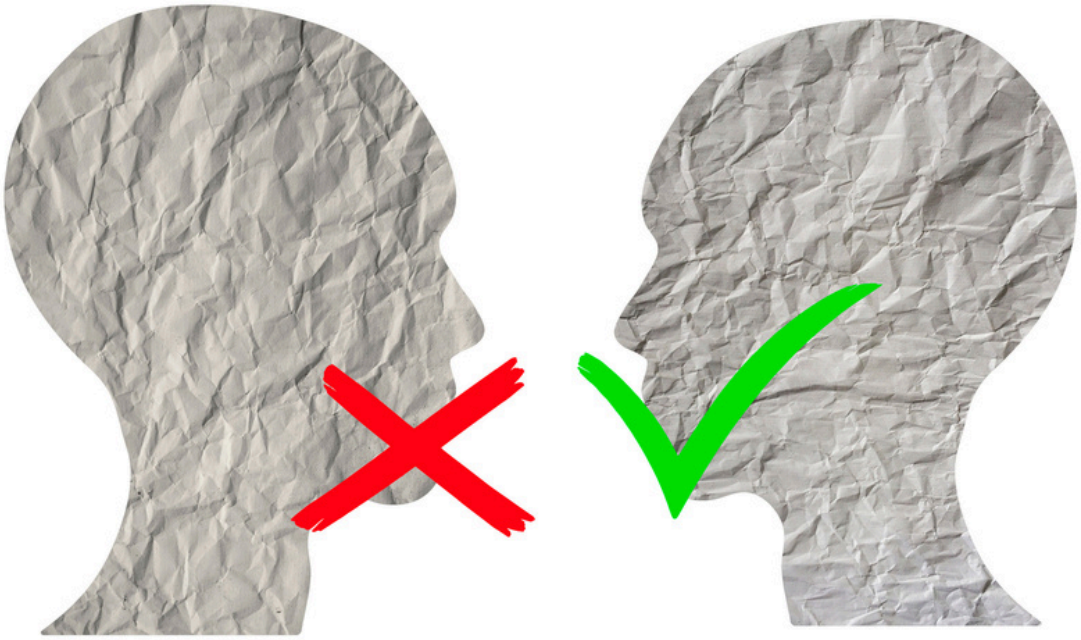
A Report from the International Foundation for Electoral Systems

Elections in the Age of Information Laws



Freedom of Expression and Information Controls in Electoral Processes

MARCH 2026

About IFES

At IFES, we envision a world where people are free, societies are democratic, and elections are fair. We collaborate with civil society, public institutions, and the private sector to build resilient democracies that deliver for everyone. As a global leader in the promotion and protection of democracy, our technical assistance and applied research develop trusted electoral bodies capable of conducting credible elections; effective and accountable governing stakeholders; civic and political processes in which all people can safely and equally participate; and innovative ways in which technology and data can positively serve elections and democracy. Since 1987, IFES has worked in more than 145 countries, from developing to mature democracies. IFES is a global, nonpartisan organization and registered as a nonprofit organization [501(c)(3)] under the United States tax code.

International Foundation for Electoral Systems

2000 M Street NW, Washington, DC, 20036, United States

www.IFES.org IFES1987

To request reprints or author engagment, please message Media@IFES.org

Elections in the Age of Information Laws

Freedom of Expression and Information Controls in Electoral Processes

AUTHOR

Nicole Leaver

Digital Democracy Specialist, IFES Center for Applied Research and Learning

PUBLISHED MARCH 2026

International Foundation for Electoral Systems

Sida

Acknowledgments

The International Foundation for Electoral Systems (IFES) extends its appreciation to the Swedish International Development Cooperation Agency (Sida) for generously supporting the development of this resource and for its commitment to strengthening democratic resilience worldwide. This research was conducted as part of a larger Sida-funded initiative on digital challenges to elections and complements the important contributions by the National Democratic Institute and the International Republican Institute.

IFES is especially grateful to our program and technical teams and regional experts in Moldova and the Philippines, whose expertise and coordination made this publication possible.

We offer our sincere thanks to the election practitioners, lawyers, academics, journalists, and civil society organizations who generously shared their experiences, insights, and time. Their courage, commitment, and daily efforts to defend and expand civic space continue to inspire and guide this work.

Contents

Abstract

In 2025, IFES conducted research on the implications of misinformation, disinformation, and malinformation laws for electoral integrity, focusing on their effects on election officials, courts, and voters. Since 2011, more than 105 such laws have been enacted worldwide, reflecting a significant global trend toward regulating online and offline speech in the context of democratic processes. While much analysis has focused on press freedom and general public discourse, limited attention has been given to how these laws affect elections and judicial processes. Drawing on a review of relevant reports, case law, and stakeholder consultations with election commissions, civil society organizations, and journalists in the Philippines and Moldova, this paper assesses how information integrity measures affect electoral institutions and human rights, and the safeguards necessary to prevent abuse.

Introduction

The proliferation of government controls on information over the past decade – specifically laws on misinformation, disinformation, and malinformation (MDM) – represents a decisive shift in the global governance of information. From 2011 to 2022, 78 countries adopted laws aimed at curbing the spread of false or harmful information.[1] A landmark study by the Center for International Media Assistance, *Chilling Legislation: Tracking the Impact of "Fake News" Laws on Press Freedom Internationally*, offers compelling evidence on how speech-regulating laws constrain media freedom. Insights from that report inform and underpin the analysis presented in this paper. While proponents of such measures argue that they are necessary to safeguard elections and preserve domestic stability, the global trend reflects increasing encroachment on freedom of expression and civic participation. Critics warn that vague definitions, overly broad enforcement mechanisms, and weak procedural safeguards have created tools for censorship and political control.[2]

These trends stand in direct tension with the international human rights framework, particularly Article 19 of the International Covenant on Civil and Political Rights, which establishes freedom of expression as both a right of individual autonomy and a cornerstone of democratic participation. Accordingly, any restriction on expression must meet a high threshold: It must be provided by law, pursue a legitimate aim, and be strictly necessary and proportionate.[3] In practice, however, many MDM laws invert this logic, treating expression as presumptively suspect and security risks as broadly defined. The erosion of Article 19 safeguards is not abstract, but rather a reshaping of the boundaries of civic space. Despite substantial scholarship on the implications of MDM laws for press freedom and public discourse, there remains a distinct lack of focused research on their impact on electoral integrity and election management body (EMB) operations.[4]

EMBs, tasked with safeguarding the integrity of electoral processes, occupy a particularly sensitive position in this evolving legal landscape. On one hand, EMBs are under pressure to counter the spread of election-related MDM that could erode trust in democratic processes and institutions. On the other, they must preserve their independence, avoid politically motivated enforcement, and protect the fundamental rights of voters, candidates, and the

---

[1] Bradshaw, S. & Lim, G. (2023). *Chilling Legislation: Tracking the Impact of "Fake News" Laws on Press Freedom Internationally*. Center for International Media Assistance. https://www.cima.ned.org/publication/chilling-legislation/

[2] Thomson Reuters Foundation & Tow Center for Digital Journalism. (2023). *Weaponizing the law: Attacks on media freedom*. https://www.trust.org/wp-content/uploads/legacy/weaponizing-law-attacks-media-freedom-report-2023.pdf; Khan, I. (2025, June 11). *Freedom of expression and elections in the digital age* (A/HRC/59/50). Office of the United Nations High Commissioner for Human Rights. https://www.ohchr.org/en/documents/thematic-reports/ahrc5950-freedom-expression-and-elections-digital-age-report-special

[3] Office of the United Nations High Commissioner for Human Rights. (n.d.). *International Covenant on Civil and Political Rights (ICCPR)*. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[4] ARTICLE 19. (2023). *Social Media 4 Peace: Content moderation and freedom of expression handbook*. https://www.article19.org/wp-content/uploads/2023/08/SM4P-Content-moderation-handbook-9-Aug-final.pdf; Bradshaw, S. & Lim, G. (2023).

media. The balance between combating harmful content and protecting democratic space has become increasingly difficult as MDM laws have proliferated. While few EMBs have the explicit mandate to regulate speech, their broad mandate to ensure free, fair, and transparent elections has increasingly been interpreted as also ensuring a healthy environment for electoral information. This implicit authority has empowered some EMBs, for instance, to issue relevant regulations, pursue collaborations with online platforms to remove content, and launch their own prebunking/debunking efforts.

Building on this premise, the analysis in this paper examines how MDM legislation and measures to counter disinformation shape EMB involvement in markedly different ways, depending on legal mandates and institutional design. In some countries, EMBs are explicitly tasked with enforcement or coordination roles related to online content, while in others their engagement arises through broader interpretations – often contested – of their responsibility to administer credible elections. Comparative evidence suggests that this ambiguity can itself become a governance risk; where responsibilities are poorly defined, EMBs may face pressure to act beyond their traditional remit, raising concerns about institutional independence and legal certainty. Accordingly, the findings do not treat countering MDM as an inherent EMB function, but analyze how varying allocations of responsibility across institutions shape key vulnerabilities (listed in the appendix) during election periods. To ground the analysis in real electoral practice, the research draws on two country-specific case studies: the Philippines and Moldova. These cases provide contrasting but comparable contexts for examining how MDM legislation reshapes EMB roles and institutional boundaries during elections.

By focusing on the electoral context, our research seeks to illuminate the real-world tensions between the stated aim of MDM legislation – combating harmful content – and the practical consequences these laws have for the independence of election authorities, the work of judicial bodies, and everyday voters' ability to participate freely in democratic processes. The findings inform a list of vulnerabilities, mapped to the electoral cycle, and offer actionable recommendations for EMBs tasked with safeguarding both electoral integrity and freedom of expression.

Global trends in MDM laws

Governments have increasingly justified MDM laws as necessary tools to protect national security, maintain public order, and ensure information integrity during crises (such as pandemics and civil unrest) and during major events such as elections.[5] In many contexts, these concerns are not unfounded; digital platforms have enabled large-scale disinformation, hate speech, and coordinated manipulation that undermine electoral participation and trust. In response, some governments and election authorities have pursued nonpunitive remedies, such as strengthening access to authoritative electoral information and partnering with civil society organizations to correct falsehoods.

[5] Bradshaw, S. & Lim, G. (2023).

For instance, the National Electoral Chamber of Argentina launched an artificial intelligence (AI)-enabled WhatsApp chatbot, named "Vot-A," ahead of the 2023 elections. Through Vot-A, voters could access a menu of electoral information services in Spanish by simply sending a greeting or scanning the QR code via WhatsApp. The chatbot, developed with Meta platform support, provided instant, up-to-date electoral information to voters, reducing confusion around voting procedures and deadlines. According to National Electoral Chamber officials, the objective was to give citizens immediate access to electoral information, thereby reducing confusion and lowering the risk of MDM.[6] This proactive, service-oriented model highlights how EMBs can use digital tools as levers to safeguard electoral integrity by empowering voters with timely, accessible, and verified data.

By contrast, many MDM laws often contain vague or overly broad provisions that can enable selective enforcement against political opponents, journalists, and civic actors.[7] These frameworks do more than regulate online content; they reshape the entire architecture of information governance. By positioning the state as the ultimate arbiter of truth, such laws can empower authorities to define credibility, police dissent, and redraw the boundaries of permissible political speech. The consequences are not abstract. As scholars have observed, individuals accused of spreading "falsehoods" often suffer immediate reputational damage – amplified by political elites or state-aligned media – long before any legal process unfolds.[8] In practice, the mere allegation becomes a tool of punishment. This dynamic hardens the asymmetry between state actors and civil society, where the power to label something as "fake" can chill debate, silence critics, and gradually constrict the democratic space that free expression is meant to protect.

Analysis of global MDM laws and practice indicate several emerging patterns, described below. These trends suggest that although MDM laws may be designed ostensibly to protect democratic processes, their broad scope and punitive mechanisms can create a fundamental structural tension with core electoral principles such as freedom of expression and political participation. As a result, EMBs, courts, and voters must operate within increasingly restrictive legal environments, particularly during high-stakes election periods.

Broad definitions and vague standards

Many MDM laws adopt expansive definitions of false information, often without clear criteria for distinguishing between intentional disinformation, unintentional misinformation, satire, and legitimate opinion. This ambiguity creates significant discretion for enforcement bodies and can chill legitimate speech.[9]

---

[6] turn.io. (2023). *CNE launches "Argentina's National Electoral Chamber 'Vot-A' chatbot: a trusted resource ahead of 2023 presidential polls"*. https://www.turn.io/news/cne-vot-a-chatbot

[7] Khan, I. (2025, June 11). *Freedom of expression and elections in the digital age* (A/HRC/59/50). United Nations Human Rights Council. https://www.ohchr.org/en/documents/thematic-reports/ahrc5950-freedom-expression-and-elections-digital-age-report-special

[8] Carson, A., & Gibbons, A. (2023). *The Big Chill? How journalists and sources perceive and respond to fake news laws in Indonesia and Singapore*. *Journalism Studies, 24*(14), 1819–1838. https://doi.org/10.1080/1461670X.2023.2192299

[9] Khan, I. (2025).

Criminalization and harsh penalties

A growing number of jurisdictions have criminalized the creation or dissemination of "false information," with penalties ranging from substantial fines to multi-year prison sentences. In several countries – including Nigeria, Tanzania, Thailand, and Vietnam – cybercrime laws have been leveraged to prosecute political speech under the guise of combating misinformation.[10]

Politicization of independent bodies

Some jurisdictions embed special provisions in their legal or regulatory frameworks that apply only during election periods, granting EMBs or other authorities elevated powers to order content removal, restrict media coverage, or sanction candidates accused of disseminating alleged falsehoods. While such measures are often defended as necessary to protect the integrity of high-stakes electoral processes, particularly in contexts of documented foreign interference or coordinated manipulation, they also carry a heightened risk of politicization if safeguards are weak or mandates unclear.

Brazil offers one of the most scrutinized examples of this model. Ahead of the 2022 general elections, Brazil's Superior Electoral Court adopted a series of resolutions empowering it to order the rapid removal of demonstrably false election-related content, suspend accounts engaged in coordinated disinformation, and impose sanctions on candidates and parties found to be spreading falsehoods.[11] At the same time, international human rights bodies and civil society organizations noted that the scope and manner of enforcement raised concerns about overreach. The United Nations Special Rapporteur on freedom of opinion and expression observed that post-election social media guidelines set by the Brazilian judiciary, while contributing to the containment of anti-democratic content, had resulted in the forced removal of a large number of posts and the blocking of social media profiles *ex officio*; in some cases, these measures had occurred through confidential decisions, limiting transparency and avenues for redress.[12]

Such tensions underscore the dual nature of election-specific enforcement powers: even when embedded in a system characterized by constitutional protections, judicial independence, and active civil society oversight, expansive takedown authority can challenge the principles of necessity, proportionality, and due process if they are not accompanied by clear standards, transparency obligations, and effective appeal mechanisms.

---

[10] Freedom House. (2024) *Freedom on the Net 2024: Nigeria*. https://freedomhouse.org/country/nigeria/freedom-net/2024; Freedom House. (2024) *Freedom on the Net 2024: Tanzania*. https://freedomhouse.org/country/tanzania; Freedom House. (2024). *Freedom on the Net 2024: Thailand*. https://freedomhouse.org/country/thailand/freedom-net/2024; Freedom House. (2024). *Freedom on the Net 2024: Vietnam*. https://freedomhouse.org/country/vietnam/freedom-net/2024

[11] Brito, R., & Boadle, A. (2022, October 20). Brazil electoral court cracks down on disinformation ahead of Lula-Bolsonaro runoff. *Reuters.* https://www.reuters.com/world/americas/brazil-electoral-court-cracks-down-disinformation-ahead-lula-bolsonaro-runoff-2022-10-20/

[12] Khan, I. (2025).

Integration with cybersecurity and defamation laws

MDM provisions are often embedded in broader cybersecurity or defamation frameworks, expanding their applicability and enforcement capacity. In some contexts, this integration facilitates rapid takedowns of violative and harmful online content during elections, but it also amplifies the risk of overreach. Nigeria offers a clear example. The country's Cybercrimes Act was introduced in 2015 to address cyber fraud and digital attacks, but has increasingly been used to investigate, arrest, or detain journalists, activists, and political commentators. Specific provisions on cyberstalking and harassment are routinely interpreted expansively, allowing authorities to pursue criminal defamation cases under the guise of countering misinformation, often without clear evidentiary thresholds.[13] Such legal layering can, in practice, expand the role of cybersecurity legislation into areas of content regulation, illustrating how integrated MDM–cybercrime frameworks can enable rapid enforcement while increasing the risk of selective application.

Cross-sectoral influence and transnational adoption

Successful (or politically expedient) models of MDM regulation are increasingly consolidated into a single legislative framework and applied across multiple domains simultaneously, rather than expanded incrementally from one sector to another. For example, Zambia's Cyber Security and Cyber Crimes Acts of 2025 combine state surveillance authorities, data governance requirements, and content-related offences, extending state oversight across telecommunications regulation, data infrastructure, and online expression.[14] As the Global Network Initiative has documented, the legislation mandates the installation of monitoring and interception facilities by service providers, imposes data localization obligations for broadly defined categories of "critical" information, and reintroduces criminal defamation provisions applicable to online speech. This consolidated model has proven influential beyond Zambia, with comparable security-driven frameworks emerging in other parts of sub-Saharan Africa, including Nigeria, Tanzania, and Uganda.[15]

Amplified risks in fragile democracies

The operational risk of MDM laws is significantly amplified in contexts already marked by institutional fragility and acute political polarization. Bolivia, for example, demonstrates how rapidly introduced speech-regulating measures can become destabilizing tools rather than safeguards, especially when adopted during moments of civil unrest or political transitions. Following the annulled 2019 elections, Bolivia was governed by a transitional administration that lacked an electoral mandate and faced widespread allegations of using state institutions to consolidate power and marginalize opposition groups. In this context, in 2020

---

[13] Zamudio-Tordecilla, G. (2023, October 26). How Anti-Cybercrime Laws Are Being Weaponized to Repress Journalism. *Columbia Journalism Review*. https://www.cjr.org/analysis/nigeria-pakistan-jordan-cybercrime-laws-journalism.php

[14] Masara, W. B. (2025, August). *How Zambia's cyber laws rebrand repression*. Journal of Democracy. https://www.journalofdemocracy.org/online-exclusive/how-zambias-cyber-laws-rebrand-repression/

[15] Global Network Initiative. (2025). GNI statement on Zambia's new cyber laws: A blow to freedom of expression and privacy. https://globalnetworkinitiative.org/gni-statement-on-zambias-new-cyber-laws-a-blow-to-freedom-of-expression-and-privacy/

the Bolivian government issued Supreme Decree 4200, and later Decree 4231, which criminalized the dissemination of misinformation regarding public health during the COVID-19 pandemic. Although the government framed Decree 4200 as a necessary emergency order, civil society organizations and the Inter-American Commission on Human Rights documented patterns of selective enforcement and intimidation, amplified by weak institutional oversight and eroding public trust.[16]

Notably, Bolivia later annulled the decree – one of the few global instances where such legislation has been successfully rolled back.[17] The rarity of this reversal underscores both the ease with which MDM legislation can be weaponized in fragile democracies and the difficulty of undoing such legislation once enacted.

Implications for election officials

MDM laws add heightened operational, legal, and reputational pressures. Although these laws are often framed as supportive tools for ensuring credible elections, their practical application can strain the principles of independence, impartiality, and transparency that underpin effective election administration.

Operational challenges

In some jurisdictions, EMBs are assigned responsibilities such as monitoring online content, issuing takedown requests, or coordinating with investigative authorities to assess alleged violations. In practice, however, EMBs are not typically the bodies that execute takedowns; removal decisions are typically carried out by platforms or, in some cases, by courts or specialized regulators.

When EMBs are tasked with initiating assessments or referrals, the timing and scope of these responsibilities can be a significant burden.[18] More specifically, MDM laws introduced shortly before an election can expand an EMB's mandate without providing the necessary lead time, budget increases, or adjustments to organizational structures. International standards emphasize that significant changes to electoral rules or administrative changes should not occur within six months of an election, because EMBs need sufficient lead time, staffing, and planning capacity to implement new mandates effectively.[19] Without these conditions, EMBs risk diverting scarce resources from core functions such as voter registration, polling logistics, and results management.

---

[16] Inter-American Commission on Human Rights. (2022). *Pandemic and human rights: Report of the Inter-American Commission on Human Rights* (OEA/Ser.L/V/II. Doc. 396/22). Organization of American States. https://www.oas.org/en/iachr/reports/pdfs/2023/pandemiaddhh_en.pdf

[17] Bradshaw & Lim (2024).

[18] Indonesia illustrates a common model in which EMBs contribute to the identification and assessment of alleged disinformation, while takedown authority rests with regulators and platforms. This upstream role can still generate operational strain and reputational risk for EMBs, particularly during compressed pre-election periods. See: Tapsell, R. (2021).

[19] Carter Center. (2014). *Election obligations and standards: A Carter Center assessment manual (2nd ed.)*. The Carter Center, https://www.cartercenter.org/wp-content/uploads/2025/08/cc-oes-handbook-10172014.pdf

Transparency and public trust

To maintain legitimacy, EMBs must balance their enforcement mandates with transparency. However, some MDM laws restrict the public disclosure of enforcement decisions, citing security or privacy concerns. This opacity can fuel suspicion among voters and stakeholders, particularly in polarized environments. As the Office of the United Nations High Commissioner for Human Rights noted in 2025, secrecy in the application of content regulation powers erodes domestic and international confidence in electoral processes.[20]

Contextual influences and global practice

EMBs increasingly navigate global policy diffusion in which legal ideas, regulatory tools, and platform governance models circulate across regions. Sharing lessons learned across jurisdictions can help strengthen electoral resilience; however, the design and institutional environment of MDM legislation can fundamentally shape its impact on a democracy. In other words, regulatory models that function under conditions of strong judicial independence may produce opposite effects when adopted in contexts marked by institutional fragility.

Germany's NetzDG framework, for example, functions within a highly institutionalized ecosystem that includes strong judicial oversight, independent data protection authorities, and well-established safeguards for freedom of expression.[21] These structural guardrails have helped ensure that content-moderation obligations placed on platforms operate within clear legal boundaries and are subject to meaningful review. In contrast, similar regulatory measures in Zambia – the country's cybercrime and cybersecurity laws – operate in a more security-driven environment where broad "fake news" provisions, extensive surveillance powers, and criminal penalties for online expression have been used against journalists and civic actors. These examples show how models that function with strong institutional safeguards can constrict civic space when they are adopted in weaker systems. International election observation missions increasingly scrutinize these dynamics, with reports emphasizing the need for EMBs to resist political instrumentalization of MDM enforcement.[22]

Implications for courts

Judiciaries play a critical role in mediating disputes arising from MDM enforcement during elections, yet they, too, face institutional and procedural challenges under these laws. In many jurisdictions, courts are the final arbiters of whether contested speech meets the

[20] Khan, I. (2025)

[21] Information Technology and Innovation Foundation (2025). *Germany's Content Moderation Regulation*. https://itif.org/publications/2025/06/02/germany-content-moderation-regulation/

[22] European Platform for Democratic Elections. (2024). *Undermining institutions: How the Kremlin involves international election management bodies in fake-observation activities*. https://epde.org/reports/new-report-undermining-institutions-how-the-kremlin-involves-international-election-management-bodies-in-fake-observation-activities/

statutory definitions of MDM, particularly when sanctions involve disqualifying candidates, restricting media, or criminal penalties.[23] The following are some key concerns:

- **Judicial independence and political pressure:** Election-related MDM cases are often politically charged, with high stakes for candidates, parties, and governance outcomes. This environment can expose judges to political pressure, particularly in systems where judicial appointments and tenure are politicized. As documented in several case studies by the Center for International Media Assistance, governments have, at times, initiated strategic litigation against opposition candidates under MDM frameworks, relying on courts to legitimize questionable enforcement actions.[24]
- **Due process concerns:** Many MDM laws grant authorities – including EMBs and various ministries – the power to impose penalties without prior judicial review, relegating courts to an appellate function. This *post hoc* review structure limits the courts' ability to prevent rights violations before they occur, and places the burden on affected parties to seek redress after electoral harm (sometimes irreparable) has already occurred.[25]
- **Evidentiary challenges:** Determining the veracity of disputed content is inherently complex, particularly in fast-moving election environments where narratives evolve rapidly. Courts must assess digital evidence, expert testimony, and fact-checking reports, often under tight electoral timelines. In some cases, courts have relied heavily on government-provided evidence without adequate opportunity for independent verification, raising concerns about impartiality.
- **Impact on electoral disputes:** The integration of MDM enforcement into electoral dispute resolution systems can expand the scope of post-election litigation. In addition to traditional vote-count challenges, courts may be called on to adjudicate claims that MDM violations affected electoral outcomes. The expanded remit of electoral dispute mechanisms raises the possibility of increased caseloads, greater strain on judicial or electoral institutions, and potential delays in certifying election results, especially when vote counts are close or contested and in contexts where disinformation could undermine confidence in preliminary outcomes.

Implications for voters

Voters are both the primary intended beneficiaries and the most vulnerable stakeholders under MDM laws applied during election periods. Such laws are often justified as safeguards against harmful falsehoods that could distort voters' decision-making process, but they can reshape the information environment in ways that reduce access to diverse perspectives, suppress legitimate political discourse, and erode trust in democratic processes.

[23] Clarke & Peoples (2023).
[24] Bradshaw, S. & Lim, G. (2023).
[25] Khan, I. (2025).

Chilling effects on political expression

When MDM laws carry criminal or severe administrative penalties, the risk of punitive action can lead citizens and journalists to self-censor political speech, especially online.[26] This chilling effect is amplified during election periods, when civic engagement intensifies and stakes are high. In Tanzania, for example, journalists reported avoiding even satirical or corrective posts after authorities began enforcing broad prohibitions on "misleading" information;[27] in Vietnam, online activists restricted commentary during the 2021 elections due to repeated arrests under Article 117 of the Criminal Code for "making, storing, or spreading information, materials, or items for the purpose of opposing the State";[28] and in Nigeria and Pakistan,[29] cybercrime provisions have been applied to critics of political figures, prompting widespread caution among reporters and ordinary citizens.

Distortion of the information environment

MDM laws can significantly shape what information reaches voters. When enforcement powers are broad, rapid takedown mechanisms may have a disproportionate impact on independent media, civil society, or opposition actors. Such distortions are especially consequential in polarized environments. Yet, as articulated above, the absence of regulation can produce its own risks. Thus, election stakeholders face a dual challenge; over-regulation can chill legitimate expression while under-regulation can enable harmful speech to flourish.[30]

Intersection with media freedom

Press freedom and voter information rights are deeply intertwined. Journalists are crucial conduits of electoral information, but MDM provisions have been used in some jurisdictions to sanction reporters and warn off critics.[31] Such actions can result in a narrowing of electoral debate and an overall decline in public scrutiny of candidates and government performance, deterring legitimate journalism for fear of prosecution or other punishment. For voters, the reduction in investigative and critical reporting diminishes the quality of electoral information.

---

[26] Carson, A., & Gibbons, A. (2023).

[27] CIVICUS. (2024). *Tanzania: End activist, media, and opposition crackdowns*. https://www.civicus.org/index.php/media-resources/news/7348-tanzania-end-activist-media-and-opposition-crackdowns

[28] Amnesty International (2021). *Viet Nam: New leadership must seize opportunity to reverse human rights decline*. https://www.amnesty.org/en/latest/press-release/2021/01/viet-nam-new-leadership-reverse-human-rights-decline/

[29] Akua, N. (2025). *How Anti-Cybercrime Laws Are Being Weaponized to Repress Journalism. Columbia Journalism Review*. https://www.cjr.org/analysis/nigeria-pakistan-jordan-cybercrime-laws-journalism.php

[30] This challenge is particularly salient as the volume of artificially generated election content increases. For a more in-depth analysis of the applications and potential impact of generative AI in election campaigns and political communications, see IFES' forthcoming report, *Generative AI in Election Campaigns and Other Political Communications: The Good, the Bad, and the Ugly.*

[31] Carson, A., & Gibbons, A. (2023).

Erosion of trust in election institutions

When voters perceive that MDM laws are applied selectively or politically, trust in the election process and its administrators can erode. This risk is especially pronounced in environments where broader constraints on civic space and expression shape public expectations about electoral fairness.

Egypt illustrates this dynamic clearly. President Abdel Fattah el-Sisi's government has expanded sweeping digital surveillance, criminalized vaguely defined "fake news," and detained journalists and citizens for online expression under the banner of national security and combating MDM.[32] In the December 2023 presidential elections, independent election monitors documented multiple structural and procedural irregularities, such as late issuance of observation permits, exclusion or harassment of viable opposition candidates, and state media practices that muted critical coverage – contributing to public perceptions that the electoral process was neither transparent nor genuinely competitive.[33] These types of broader information and media controls can reinforce a narrative of predetermined outcomes and narrow choice, undermining confidence in both the results and the institutional neutrality of election authorities.

Digital literacy and civic agency

Punitive approaches to MDM often operate in parallel with – rather than in support of – voter education and digital literacy efforts. This creates a structural imbalance; restrictive laws may criminalize or suppress certain kinds of speech, but they rarely invest in the civic competencies that enable voters to critically assess the information in the first place. In some contexts, civil society organizations report that even nonpartisan voter education efforts risk being scrutinized under broad MDM laws, particularly when they involve fact-checking political claims or explaining contested electoral issues.[34]

In contrast, Taiwan offers a notable example of how regulatory frameworks can embed digital literacy as a central pillar of electoral resilience. Under its broader digital democracy and information integrity initiatives, the government funds nationwide media literacy curricula, supports community fact-checking networks such as the Taiwan FactCheck Center, and deploys participatory civic technology tools, including government chatbots, to provide rapid, verified electoral information.[35] These efforts demonstrate that empowering voters can be a more sustainable strategy for mitigating falsehoods during elections.

---

[32] Mansour, S. (2018). Censorship tightens in Egypt as el-Sisi prepares for re-election bid. *Committee to Protect Journalists*. https://cpj.org/2018/03/censorship-tightens-in-egypt-as-el-sisi-prepares-f/

[33] Egyptian Front for Human Rights (2024). *The path to the presidential palace: Monitoring and evaluation report of the Egyptian presidential elections 2023*. https://egyptianfront.org/2024/03/the-path-to-the-presidential-palace-monitoring-and-evaluation-report-of-the-egyptian-presidential-elections-2023/

[34] Article 19. (2023).

[35] Barron, D. (2025). *Taiwan's model for digital defense of democracy goes global*. The Diplomat. https://thediplomat.com/2025/06/taiwans-model-for-digital-defense-of-democracy-goes-global/

Case Studies: The Philippines and Moldova

This section introduces two comparative case studies that ground the analysis in real electoral practice. The Philippines and Moldova illustrate how different legal, political, and institutional environments shape the application of MDM regulation and the role of EMBs. Together, these cases provide empirical context for assessing the risks, safeguards, and institutional dynamics discussed throughout the report.

Rationale for case study selection

The Philippines and Moldova were selected as significant comparative case studies due to their shared experience in managing the increasingly complex role that MDM regulation plays in contemporary elections. In each case, regulatory interventions were introduced or applied in response to genuine concerns, including foreign interference, large-scale manipulation, and the documented harms of MDM on their electoral processes, political participation, and marginalized groups. Recent global human rights reporting has underscored that electoral disinformation now operates across the full electoral cycle, often beginning long before polling day and persisting well after the election results are announced.[36]

At the same time, both cases demonstrate the risks that arise when speech-regulating frameworks are operationalized during high-stakes electoral periods. As comparative research has shown, not all approaches to combating MDM have negative consequences; measures such as platform transparency requirements, investments in media literacy, and support for independent journalism can strengthen democratic resilience.[37] However, many recent regulatory responses – particularly those centered on criminal sanctions or emergency powers – have introduced risks of selective enforcement, self-censorship, and politicization even when adopted with legitimate security objectives in mind.

In the Philippines, this tension is visible in the interaction between criminal speech provisions, such as those in the Cybercrime Prevention Act and election-specific regulatory measures issued by the Commission on Elections (COMELEC). In Moldova, similar dynamics emerge through legislation empowering the Intelligence and Security Service (SIS) and the Audiovisual Council to intervene in online content and media monitoring during electoral periods. IFES observed both elections, gathering timely data on how these frameworks functioned in practice and how enforcement choices shaped the operating environment for EMBs, media actors, and civil society.

Finally, international freedom of expression indexes reveal difficulties in protecting digital civic space in both countries, with Freedom House's 2024 *Freedom on the Net* rankings both designating Moldova and Philippines as "partly free."[38] This shared challenge of balancing national security concerns and election integrity with constitutional protections for

[36] Khan (2025).
[37] Bradshaw and Lim (2024).
[38] Freedom House. (2024). *Moldova: Freedom in the World 2024 country report*. https://freedomhouse.org/country/moldova/freedom-world/2024; Freedom House. (2024). *Philippines: Freedom on the Net 2024 country report*. https://freedomhouse.org/country/philippines/freedom-net/2024

expression makes them ideal country-specific examples for analyzing effective safeguards for EMBs globally.

Case study: The Philippines

The Philippines offers a complex and highly instructive case of how MDM laws intersect with election administration, press freedom, and political polarization. The legal framework governing online speech in the Philippines – including the Cybercrime Prevention Act of 2012 and criminal libel provisions under the Revised Penal Code – is fragmented, punitive, and unevenly enforced. Election-specific provisions, most prominently COMELEC Resolution No. 11064, add another layer of regulation aimed at curbing digital manipulation and AI-generated content. These interventions exist alongside deeply entrenched political patronage networks, red-tagging practices,[39] and a commercialized disinformation industry, all of which frustrate attempts to distinguish legitimate electoral safeguards from the political weaponization of speech controls.

Against this backdrop, IFES led a research mission to gather data and insights during the 2025 general elections in the Philippines. The following observations are based on analysis of comprehensive desk research and primary interviews with COMELEC, civil society organizations, journalists, and academics.

Overview

The 2025 Philippine general elections were shaped by the entrenched rivalry between the Marcos and Duterte political dynasties. While political competition was intense, the broader legal and digital environment for free expression remained both under-regulated and aggressively enforced. Stakeholders described a regulatory environment in which laws intended to counter harmful speech often failed to address structural drivers of manipulation while enabling targeted suppression of journalists, activists, and critics. The roots of this ecosystem stretch back to the authoritarian rule of Ferdinand Marcos, Sr. (1965–1986), during which a state-run propaganda apparatus normalized strategic information control and crafted narratives that continue to animate political discourse today.

Under Rodrigo Duterte's presidency (2016–2022), these practices modernized into a commercialized digital influence industry built on political patronage networks linking politicians, public relations firms, and paid influencers.[40] This history has entrenched patterns of authoritarian nostalgia, coordinated propaganda, and the tactic of red-tagging

---

[39] Red-tagging is defined as "labeling individuals or organizations as communist sympathizers or terrorists without substantial evidence." This label can carry serious consequences, such as harassment, political exclusion, and, in extreme cases, physical violence and death. For additional context, see: Gupta, S. (2024). *Red-Tagging in the Philippines: The Modern McCarthyism Threatening Freedom of Expression*. Global Freedom of Expression, Columbia University. https://globalfreedomofexpression.columbia.edu/publications/red-tagging-in-the-philippines-the-modern-mccarthyism-threatening-freedom-of-expression/

[40] Sigla Research Center. (2025). *2025 Elections Report*. https://siglaresearch.org/news-and-events/2025-elections-report/

critics as communist sympathizers, all of which complicate efforts to distinguish legitimate regulation of harmful content from politically motivated suppression during elections.

By 2025, the regulatory landscape governing speech and online communications was defined by a combination of old and new digital regulations. The Cybercrime Prevention Act of 2012, widely used to file cyber libel complaints against journalists, remained a significant pressure point for independent media and attracted global attention following the arrest of high-profile journalist Maria Ressa.[41] In 2020, the Anti-Terrorism Act expanded state surveillance powers and enabled warrantless detention, raising persistent concerns about arbitrary application.[42] Shortly afterwards, the SIM Registration Act (2022) introduced mandatory ID verification for SIM activation, aimed at curbing scams, which heightened surveillance risks in a politically sensitive environment.[43]

Against this backdrop, COMELEC Resolution No. 11064 (2024) marked an ambitious attempt to regulate digital campaigning. The resolution mandated registration of digital campaign platforms, required disclosure of AI-generated content, restricted coordinated inauthentic behavior, and granted the Commission authority to order takedowns.[44] Although it improved transparency and increased cooperation from technology companies, stakeholders consistently noted ambiguous definitions, uneven enforcement, and a lack of independent oversight.

Consultations with local stakeholders, including the Alliance for Media Alternatives, LENTE, COMELEC, Sigla Research Center, ABS-CBN, and international partners, highlighted both progress and systemic challenges. Interlocutors emphasized that although COMELEC had made notable strides in engaging platforms and setting expectations for digital campaigning, there was an urgent need for stronger safeguards against politicized enforcement, clearer definitions of disinformation, and protections for journalistic and public interest speech.

With the rapid rollout of satellite internet services such as Starlink, detailed below, COMELEC faces new jurisdictional and enforcement challenges that could either expand civic participation or exacerbate the risks of microtargeting, surveillance, and voter suppression. The next three years offer a critical window to ensure that regulatory

---

[41] BBC (2020). *Maria Ressa: Philippine journalist found guilty of cyber libel*. https://www.bbc.com/news/world-asia-53046052

[42] Sobel, A. (2020). *The Philippines' Antiterror Bill Will Stifle Dissent*. Carnegie Endowment for Democracy. https://carnegieendowment.org/posts/2020/06/the-philippines-antiterror-bill-will-stifle-dissent?lang=en

[43] In several interviews, stakeholders conveyed that the SIM Registration Act was not a genuine attempt to clamp down on cybercrime, but rather a measure to further expand surveillance powers. They noted that people were pushing back on mandatory registration in various ways and highlighted the popular example of an individual successfully using the a monkey's photo to register a SIM card. Rappler (2023). *Monkey's photo passes in SIM card registration in Philippines*. https://www.rappler.com/business/monkey-photo-register-sim-card-registration-philippines/

[44] Digital Policy Alert. (2025). *Philippines: Implemented COMELEC guidelines on the use of social media, artificial intelligence and internet technology for the 2025 elections and the BARMM parliamentary elections*. https://digitalpolicyalert.org/event/23504-implemented-comelec-guidelines-on-the-use-of-social-media-artificial-intelligence-and-internet-technology-for-the-2025-elections-and-the-barmm-parliamentary-elections

frameworks are ahead of the curve by strengthening freedom of expression, establishing robust AI governance frameworks, and ensuring that digital regulation enhances democratic integrity, rather than eroding it.

Implementation of Resolution No. 11064

The implementation of Resolution No. 11064 revealed a mix of progress and persistent structural tensions in the Philippines' evolving information-regulatory landscape. On one hand, the effort produced several encouraging developments: Candidates' compliance with the platform registration requirement was notably high; COMELEC succeeded in establishing cooperative protocols with major technology companies; and public-facing campaigns helped raise awareness about manipulated media and AI-generated content.[45] According to ANFREL observers, these steps reflected the Commission's genuine efforts to introduce greater transparency in digital campaigning and confront the scale of information manipulation that now characterizes every Philippine election cycle.

Yet, rollout of the resolution exposed significant challenges, suggesting that the regulatory architecture had yet to find stable footing. Many civil society organizations expressed unease about the discretionary nature of enforcement, especially provisions that could be interpreted as covering the personal accounts of ordinary citizens. Responding to this pressure, COMELEC revised the resolution in November 2024 to explicitly narrow its application to official candidate accounts, clarifying that individual users would not be required to register their personal social media pages.[46] This revision is widely viewed as an important lesson learned, underscoring both the value of public consultation and the need for careful calibration when regulating online political expression.

While recognizing these strides, stakeholders reported that enforcement remained uneven across regions, with local COMELEC offices varying in capacity, staffing, and operational preparedness. In particular, concerns about discretionary decision-making were raised, including that the boundary between disinformation, satire, and legitimate criticism remains thin and poorly defined – a condition that can contribute to self-censorship among journalists and opposition groups.[47]

Structural gaps in accountability compounded these concerns. There is no independent or impartial body to review takedown orders or question COMELEC's determinations, leaving affected candidates or organizations without a credible avenue for appeal. Finally, the integration of SIM registration data into compliance and enforcement workflows introduced new layers of surveillance anxiety, particularly among journalists, activists, and smaller

---

[45] Baker McKenzie. (2024, October 4). *Philippines: AI and social media guidelines for the 2025 elections issued by the COMELEC.* InsightPlus. https://insightplus.bakermckenzie.com/bm/data-technology/philippines-ai-and-social-media-guidelines-for-the-2025-elections-issued-by-the-comelec

[46] ANFREL (2025). *Interim Report of the ANFREL International Election Observation Mission to the 2025 Philippine national and local elections.* https://anfrel.org/interim-report-of-the-anfrel-ieom-to-the-2025-philippine-elections/

[47] ANFREL (2025).

political actors who already operated in a climate of digital intimidation.[48] Taken together, these dynamics underscore that although Resolution No. 11064 represents an important first attempt at governing AI and online political communication, its implementation has exposed the need for clearer definitions, stronger safeguards, and more robust oversight mechanisms.

Patterns of overreach and institutional constraints

While noting that Resolution No. 11064 enhanced transparency in digital campaigning, its implementation revealed several practical and reputational pressures on COMELEC. Interviews and findings from ANFREL's interim observation report indicate that the Commission operated in an unusually crowded enforcement environment, where responsibilities for online content were shared informally, sometimes inconsistently, with law enforcement, the military, and agencies involved in counterterrorism and cyber operations. This overlap created uncertainty about which institution was actually responsible for investigating disinformation and issuing sanctions, leaving some stakeholders with the perception that COMELEC's decisions may have been influenced by, or tethered to, security-sector priorities rather than purely electoral integrity considerations.

In operational terms, civil society organizations noted that the Commission's reliance on external agencies for verification or technical assistance introduced delays and, in some cases, reduced the transparency of the decision-making process. Such bottlenecks can introduce barriers to performing core election functions, particularly during a compressed pre-election period.

Stakeholders also emphasized the risk to perceived independence. In a political environment where "fake news" laws and cyber-libel prosecutions are routinely used by state actors, any appearance that COMELEC was aligned with security agencies could heighten public suspicious, even if the Commission is acting within its mandate. For example, Sigla Research Lab documented instances where takedown decisions were announced without sufficiently detailed public explanations, prompting speculation among journalists and small political parties about selective enforcement.

At the same time, COMELEC did respond to public concerns about transparency. In an interview for this research effort, ABS-CBN applauded COMELEC for visiting newsrooms and meeting with journalists in the lead-up to the election. And, as detailed above, after pressure from civil society, the Commission amended the resolution to narrow its scope – a change that was widely viewed as a corrective measure that both reduced operational burden and mitigated perceived risks to independence.

Ultimately, interlocutor interviews indicated that although COMELEC had engaged constructively and in good faith to operationalize the resolution, the absence of clearly defined institutional boundaries, independent avenues for appeal, and adequate resourcing

[48] Mozilla. (2022, April 5). *Philippines SIM card-registration act will expose users to greater privacy and security risks online*. Mozilla Policy Blog. https://blog.mozilla.org/netpolicy/2022/04/05/philippines-sim-card-registration-act-will-expose-users-to-greater-privacy-and-security-risks-online/

placed the Commission under considerable operational and reputational strain. These observations point to an opportunity for future regulatory frameworks to more explicitly delineate enforcement roles and accompanying safeguards to effectively support COMELEC.

Looking forward: risks and opportunities

The Philippines, with its entrenched disinformation networks and a legal environment that frequently relies on punitive tools, faces a critical juncture ahead of the 2028 election cycle. COMELEC officials emphasize that MDM – particularly false narratives targeting election logistics, digital impersonation of official communications, and AI-enabled manipulation – pose real operational risks during elections. Similarly, interlocutors expressed concern about continuing tensions between criminal enforcement actions and broader efforts to strengthen digital governance, such as greater investment in local newsrooms and civic education.

Emerging discussions across civil society organizations have underscored interest in shifting toward nonpunitive information integrity models that distribute responsibility across institutions, platforms, and communities. Grassroots digital literacy initiatives (such as fact-checking partnerships) and accountability mechanisms were frequently cited as potential avenues for mitigating influence operations. These include norm-based commitments by political actors, civil society fact-checking groups, and major technology companies. In our discussions with COMELEC, they often cited IFES' *Voluntary Election Integrity Guidelines for Technology Companies* as an influential roadmap for engaging with social media platforms.[49]

At the same time, Filipino journalists expressed concern about platform retrenchment and warned that Meta's recent shift in fact-checking operations and reducing support in the Global South could weaken the country's information resilience efforts in future elections. This aligns with broader international research showing that fragmented platform governance and competing national tech sovereignty strategies leave democracies with uneven protections against digital manipulation.[50] In practice, global technology companies apply different standards across markets, meaning well-designed domestic approaches cannot fully compensate for insistent or insufficient platform cooperation. In the Philippines, the integrity of the information environment is shaped not only by domestic law or COMELEC's capacity, but also by platforms' level of cooperation and investment across the region. Democracies without strong regulatory leverage, or those located in what platforms categorize as "lower-priority" markets, could be more vulnerable to digital manipulation simply because global platform governance is unequal by design.[51]

---

[49] IFES. (2024). *Voluntary Election Integrity Guidelines for Technology Companies*. https://electionsandtech.org/election-integrity-guidelines-for-tech-companies/

[50] Feldstein, S, ed. (2025). *Digital Democracy in a Divided Global Landscape*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/05/digital-democracy-in-a-divided-global-landscape?lang=en

[51] Feldstein, S, ed. (2025).

Finally, the 2025 rollout of Starlink in areas underserved by digital infrastructure, as announced by President Ferdinand Romualdez Marcos Jr., promises to expand digital participation – but presents new governance challenges.[52] Satellite networks may bypass domestic enforcement mechanisms, complicating takedown protocols and platform registration compliance. The integration of satellite services introduces jurisdictional and oversight questions that could reshape how regulatory agencies enforce election period rules or manage data governance concerns and, as a result, lead to increased risks to privacy and surveillance, particularly in rural and conflict-affected communities.

Across these areas, one theme was consistent: managing digital threats requires a layered, whole-of-society model of information governance.[53] How these components evolve and whether institutional investment keeps pace will shape the Philippines' ability to maintain a transparent, rights-respecting information environment in upcoming electoral cycles.

Case study: Moldova

Moldova offers a particularly salient example of how quickly MDM legislation is being folded into electoral processes. Long positioned as the geopolitical crossroads between the European Union and Russia, the country has faced sustained pressure on its information environment, leaving institutions to manage not only routine electoral administration, but also persistent attempts of foreign interference. Against the backdrop of Russia's war on neighboring Ukraine, policymakers have increasingly framed information regulation as an urgent national security priority.

Stakeholders described the 2025 parliamentary elections as marred by serious cases of foreign interference, illicit financing, cyberattacks, and widespread disinformation. The overlapping pressures created an environment in which security imperatives and electoral integrity became tightly intertwined, blurring the line between legitimate protective measures and potential overreach.

Overview

In March 2024, the Moldovan parliament approved amendments to its Contravention Code and Criminal Code, imposing fines for the dissemination of false information online, framed as part of a broader national security strategy.[54] These measures were enacted in the context of alleged and documented foreign interference targeting the country's democratic institutions and its path toward European Union integration.[55] Moldovan authorities

---

[52] Philippine News Agency. (2025, January 28). *Provisional authority for Starlink to bridge digital divide in PH*. https://www.pna.gov.ph/index.php/articles/1242786

[53] Donovan, J., et al. (2021). *Mitigating Medical Misinformation: A Whole-of-Society Approach to Countering Spam, Scams, and Hoaxes*. The Media Manipulation Casebook. https://casebook-static.pages.dev/research/mitigating-medical-misinformation-whole-society-approach-countering-spam-scams-and-hoaxes/

[54] CSO Meter. (2025). *Moldova: New proposal to impose fines for online disinformation.* https://csometer.info/updates/moldova-new-proposal-impose-fines-online-disinformation

[55] OSCE Parliamentary Assembly. (2025). *Moldova's parliamentary elections were competitive but campaign marred by cyberattacks, illegal funding and disinformation, international observers say* [Press release].

presented this regulatory turn as a defensive necessity rather than a discretionary choice, yet its rapid adoption also raised questions about proportionality, institutional preparedness, and the risks of normalizing emergency-style governance.

The CEC is not the primary enforcement authority for MDM-related sanctions, but its mandate to administer elections and protect electoral infrastructure requires close coordination with Moldova's Intelligence and Security Service (SIS) and Information Technology and Cyber Security Service (STISC). This cooperation has focused primarily on safeguarding voter databases, results transmissions systems, and official digital platforms from cyberattacks.

Many interlocutors acknowledged that such collaboration is both necessary and, in several respects, effective. At the same time, in IFES' interviews with media organizations, stakeholders emphasized that the lack of publicly accessible documentation clearly delineating roles for the CEC, SIS, and STISC has contributed to unease. In particular, the absence of public-facing documentation explaining their operational mandates – specifically whether the CEC is substantively depending on STISC for any elements of voter data management, security protocols, or results transmission – has reinforced concerns. In interviews, stakeholders repeatedly noted that uncertainty is itself corrosive; when organizational transparency is substituted with assumptions, trust inevitably erodes.

Operational pressures amplified these tensions. As new MDM measures heightened expectations for the rapid correction of false narratives, the Commission simultaneously faced targeted disinformation campaigns, including a cloned CEC website and attacks on its chairperson. Cybersecurity company Cloudflare reported that the CEC was hit by a coordinated, 12-hour distributed denial-of-service attack on election day, generating more than 898 million malicious requests.[56] Complex cybersecurity pressures do not occur in a vacuum; rather, they compound one another, creating an environment where an already resource-strained institution must react simultaneously to operational and reputational threats.

Layered atop cybersecurity attacks, the CEC faced intense and highly consequential judicial scrutiny. Decisions by the Commission and the Chişinău Court of Appeals issued shortly before election day revoked the eligibility of two parties, including the Heart of Moldova Party (PRIM), citing serious campaign finance violations.[57] The rulings targeted foreign interference and illicit financing, but their last-minute timing undermined legal certainty and limited the

---

https://www.oscepa.org/en/news-a-media/press-releases/2025/moldovas-parliamentary-elections-were-competitive-but-campaign-marred-by-cyberattacks-illegal-funding-and-disinformation-international-observers-say

[56] Cloudflare. (2025, October 29). *Helping protect the 2025 Moldova elections*. https://blog.cloudflare.com/helping-protect-the-2025-moldova-elections

[57] Gjevori, E., & News Agencies. (2025, September 26). *Moldova bans pro-Russian parties ahead of Sunday's election*. Al Jazeera. https://www.aljazeera.com/news/2025/9/26/moldova-bans-pro-russian-parties-ahead-of-sundays-election

parties' window for meaningful appeal, prompting concerns from international observers.[58] Although these decisions were not taken under the new MDM provisions, they unfolded in a legal and political context where disinformation, external manipulation, and national security had become central frames for electoral governance. As a result, voters and political actors encountered a compressed sequence of enforcement actions spanning campaign finance rules, information controls, and security measures.

Stakeholders interviewed by IFES noted that when MDM enforcement, financial sanctions, and security measures converge late in an election cycle, the CEC's actions are more likely to be viewed through a single, securitized lens, regardless of their legal grounding. What becomes clear across these dynamics is that even well-grounded institutional actions can become destabilizing when executed under intense time pressure and without transparency or robust safeguards for due process. The CEC is navigating an environment in which it must protect the integrity of elections while defending itself from digital attacks, fabricated political narratives, and judicial decisions that can rapidly reshape the electoral landscape.

Without strengthened transparency, clearer delineation of institutional mandates, and more predictable enforcement timelines, the CEC risks being caught in the crossfire as both a steward of the democratic process and an unintended instrument in broader political struggles. To mitigate these risks, stakeholders pointed to a need for greater procedural transparency around information-related decisions (such as publishing reasoned explanations for content referrals, website blocking requests, or coordination with security agencies) to help distinguish MDM-related actions from other enforcement measures. Even when operational details cannot be disclosed, outlining the decision-making criteria, responsible authority, and applicable legal framework could strengthen public understanding and accountability.

Legal environment

Moldova's current MDM framework reflects a gradual shift toward emergency-style information governance that has unfolded over several years rather than as a single legislative break. Early precedents emerged during the COVID-19 pandemic, when authorities relied on emergency powers to address MDM related to public health, normalizing the idea that misleading content could justify exceptional administrative restrictions in the name of public order. These early measures established a pattern in which information harms were framed less as media or regulatory challenges and more as security threats requiring rapid state intervention.

This approach deepened following Russia's full-scale invasion of Ukraine in 2022, as Moldova faced heightened concerns over foreign interference, hybrid threats, and destabilization efforts linked to its European Union accession trajectory. Amendments to the Code of Audiovisual Services in 2022 expanded the definition of "disinformation" and

[58] OSCE Office for Democratic Institutions and Human Rights. (2025, March 14). *Election Observation Mission: Republic of Moldova – Parliamentary Elections, 28 September 2025*. https://odihr.osce.org/sites/default/files/f/documents/4/7/597800_0.pdf

increased regulators' discretionary authority to impose sanctions, particularly in broadcast media. By 2024, further amendments to the Contravention Code and Criminal Code codified administrative penalties for the dissemination of "false information" deemed harmful to national security or public order. These provisions, presented as defensive and temporary safeguards, embedded security logics directly into the legal architecture governing speech, blurring the line between emergency response and ordinary regulation.

The new provisions defined "false information" broadly, allowing for administrative penalties against individuals and media outlets that disseminated unverified content deemed harmful to national security or public order.[59] Amendments to the Code of Audiovisual Services, introduced in 2022, also broadened the definition of "disinformation" and expanded the sanctioning authority of the Audiovisual Council, enabling it to impose administrative penalties, including fines and license suspensions, on broadcast media. This approach, as election stakeholders that IFES interviewed warned, risks blurring the lines between harmful content and valid political critique, allowing for the potential for selective enforcement.

The law's scope extends to online platforms, obligating them to cooperate with state authorities in identifying and removing content. In practice, this framework has enables expedited takedown requests and website blocking decisions, frequently implemented without advance notice to affected outlets or a clear public explanation of their legal basis and duration. The *CSO Meter: 2024 Moldova Country Report* observes that rapid, nonconsultative legal amendments, often justified on national security grounds, can create instability and weaken the predictability of the legal environment for media and nongovernmental organizations.[60] Over time, this uncertainty risks undermining confidence in both the consistency of information governance and the institutions responsible for administering it.

Patterns of overreach and institutional constraints

Moldova's legal ecosystem grants wide discretion to executive and security bodies. Between 2022 and 2023, under opaque emergency information-security measures, the Audiovisual Council suspended the licenses of at least 12 broadcasters, many linked to the pro-Șor party (a major opposition party).[61] These actions were justified as necessary to counter foreign interference, including documented illicit Russian financing channeled through entities associated with Ilan Șor, whose party was formally banned in 2023 following extensive investigations into election interference and financial crimes.[62] In the aftermath of the ban, observers and civil society organizations reported that Șor-linked funding did not disappear

[59] CSO Meter. (2025).
[60] Promo-LEX Association. (2024). *CSO Meter: Moldova 2024 Country Report*. https://csometer.info/sites/default/files/2025-02/CSO%20Meter%20Moldova%202024_ENG.pdf
[61] Amnesty International. (2025, November 17). *Moldova: Fragile media challenged by vague laws, undue sanctions and harassment*. https://www.amnesty.org/en/latest/news/2025/11/moldova-fragile-media-challenged-by-vague-laws-undue-sanctions-and-harassment
[62] BBC (2023). *Moldovan court bans pro-Russian party Sor. https://www.bbc.com/news/world-europe-65952878*

but was instead dispersed among smaller parties, media outlines, and online platforms, complicating attribution and enforcement.

While these interventions responded to well-substantiated threats, the absence of publicly articulated criteria, timelines, and appeal mechanisms raised concerns among media stakeholders about selective enforcement and legal predictability. Specifically, election stakeholders emphasized that the SIS has operated with broad and poorly supervised authority to block websites even outside of emergency decrees, contributing to an environment of legal ambiguity. Since 2020, an estimated 50 sites have been blocked, with minimal public oversight.[63] In IFES' conversations with local organizations, many expressed frustration that the public often learns about these decisions *post hoc*, with little ability to challenge or understand the underlying rationale.

Many of the individuals that IFES spoke to expressed fatigue, resignation, and a sense of operating under constant uncertainty. The absence of pathways to appeal decisions or effective remedies to reinstate websites, for instance, leaves civil society and media organizations with virtually no resources if they are unfairly targeted. These actions contribute to a troubling dynamic seen not only in Moldova, but around the world; the tools intended to protect the information environment are often deployed through processes that lack transparency, proportionality, and due process. As a result, well-intentioned safeguards risk sliding into mechanisms of censorship.

Looking forward: risks and opportunities

Generative AI has compounded disinformation challenges well beyond the reach of Moldova's existing institutional and legal frameworks, enabling influence operations at a scale and speed that regulators were neither equipped nor mandated to address. In the lead-up to the election, an undercover investigation led by the BBC and Ziarul de Gardă revealed a Moscow-linked "digital army" of more than 250 inauthentic accounts across TikTok, Facebook, and Instagram.[64] Additional monitoring by civil society organization Promo-LEX identified a sprawling network of more than 500 accounts producing fabricated endorsements, deepfakes, and coordinated falsehoods related to Moldova's European integration.[65] These campaigns demonstrate not only the tactical use of generative AI for manipulation, but also the growing professionalization of foreign influence operations, which increasingly mirror formal digital marketing ecosystems in targeting strategies and multilingual support. Critically, these networks have operated with a level of automation and narrative discipline that far outpaced the ability to respond in real time, illustrating how easily malign actors can exploit the asymmetry between state capacity and adversarial innovation.

---

[63] International Press Institute. (2020, March 20). *Moldova: Authorities issue takedown orders on 52 websites accused of spreading "fake news."* https://ipi.media/alerts/moldova-authorities-issue-takedowns-orders-on-52-websites-accused-of-spreading-fake-news/; Amnesty International. (2025, November 17).

[64] DFRLab. (2025, September 24). *Paid to post: Russia-linked 'digital army' seeks to undermine Moldovan election*. DFRLab. https://dfrlab.org/2025/09/24/paid-to-post-russia-linked-digital-army-seeks-to-undermine-moldovan-election/

[65] Promo-LEX. (2025, September 19). *Massive online networks that manipulate voting*. https://promolex.md/en/massive-online-networks-that-manipulate-voting

These digital threats exist alongside growing concerns about the impact on civic space. Representatives from one organization that IFES interviewed alleged that the SIS processed more than 2 million citizen data queries via the MConnect data exchange platform, raising fears of function creep and intrusive data practices by security agencies.[66] Such practices can weaken public trust in an environment lacking transparent oversight mechanisms that would support voters' visibility into how their data is being accessed or shared. Civil society actors repeatedly emphasized that the line between necessary security coordination and expansive surveillance is becoming increasingly difficult for the public to discern. This ambiguity risks chilling speech, suppressing dissent, and deepening societal divisions.

Despite these challenges, civil society organizations such as Promo-LEX and WatchDog MD have continued to play a critical watchdog role in documenting election violations and exposing covert influence operations. In some respects, the introduction of MDM-related provisions has created limited new entry points for civil society to challenge demonstrably false narratives and draw attention to coordinated manipulation. At the same time, organizations consistently reported that broad and imprecise legal definitions of "false information" have contributed to heightened caution, particularly when reporting on sensitive topics related to national security, foreign interference, or state institutions. This has raised concerns about indirect self-censorship, even among experienced monitoring groups.

These pressures are compounded by a widening gap between the scale and sophistication of digital threats and the resources available to independent watchdogs. Civil society actors emphasized that as expectations for monitoring and rapid response have increased, access to platform data, sustainable funding, and formal coordination mechanisms have not kept pace. Cross-sectoral cooperation is often operationally necessary, but stakeholders cautioned that overreliance on external security bodies, without clear protocols and transparency, can further entrench asymmetries between state institutions and independent oversight actors. Without predictable funding, meaningful data access, and institutionalized channels for engagement, civil society organizations risk remaining structurally disadvantaged in an environment where malign actors benefit from speed, scale, and opacity.

Future reforms should aim to ensure that any legal and institutional responses to MDM remain narrowly tailored, transparent, and consistent with international human rights standards. For the CEC, this includes addressing capacity constraints that have practical implications for institutional independence. Stakeholders observed that when election commissions lack sufficient internal expertise or staffing to manage complex information threats, reliance on security and intelligence agencies can increase by default, rather than by design. Over time, this dynamic risks shaping both public perception and internal decision-making in ways that may unintentionally blur the CEC's independence and expose it to perceptions of politicization at critical moments in the electoral cycle.

[66] IFES has not been able to independently verify this claim.

To build public trust and ensure due process, future reforms may increasingly hinge on strengthening both judicial and regulatory mechanisms, not the courts alone. This includes clearer administrative procedures and pathways within the bodies responsible for content removals, website blocking, and media regulation. Current law does not provide for the removal of candidates solely on the basis of spreading disinformation; nonetheless, the timing and visibility of MDM-related enforcement actions (including fines, broadcaster suspensions, or website blocking) can shape the electoral information environment in ways that affect political competition. When such measures are applied late in the electoral cycle or without clear public explanation, they risk creating perceptions of arbitrariness even when formal legal thresholds are met.

Sustained support for civil society and media literacy is likely to remain a central component of societal resilience in the face of rapidly evolving AI-generated influence operations. Yet, it is difficult to ignore that civil society is increasingly expected to confront large-scale, well-resourced digital manipulation with comparatively limited access, funding, or technical capacity. A forward-looking approach therefore suggests that alongside legal safeguards, structural investment in CSO capacity, access to platform data, and formalized engagement channels with regulators is necessary to ensure that MDM laws strengthen independent oversight of the information environment. Without addressing the widening resource gaps, the durability of Moldova's democratic safeguards may remain contingent on actors that are systemically under-resourced relative to the challenges they are tasked to confront.

Recommendations for election management bodies: safeguarding free expression and election integrity

The following recommendations are intended to support EMBs in navigating the evolving relationship between election integrity, freedom of expression, and information controls, particularly in the contexts shaped by MDM legislation. They are informed by commitments by the Organization for Security and Co-operation in Europe (OSCE)[67] and guidelines from the Global Network for Securing Electoral Integrity (GNSEI),[68] and focus narrowly on strengthening EMBs' independence and impartiality.

1. Clearly define and publicly communicate the election management body's mandate in the electoral environment.

EMBs should formally articulate the scope and limits of their role with respect to election-related information, particularly where MDM frameworks are in force. Providing public clarification that the EMB's mandate relates to election administration and the provision of official electoral information, rather than adjudicating political speech, can bolster institutional independence and mitigate perceptions of partisan enforcement. For example, an EMB may seek to establish memoranda of understanding outlining roles and responsibilities and to integrate state–agency interactions in its strategic communications plan.

This approach aligns with GNSEI's guidance on clarifying mandates to strengthen systematic planning and prevent undue interference from other public institutions.

2. Prioritize the provision of authoritative electoral information as the primary response to misinformation, disinformation, and malinformation.

EMBs should focus on proactively disseminating accurate, timely, and accessible information regarding electoral procedures, timelines, and requirements, particularly during periods of heightened risk or crisis. When false or misleading claims arise that could jeopardize voters' participation or confidence, EMBs should respond through public clarification rather than seeking punitive measures.

This recommendation aligns with the OSCE standards emphasizing voters' right to access information and EMBs' responsibility to facilitate informed participation, as well as GNSEI guidance encouraging transparency and proactive communication as confidence-building measures.

---

[67] Organization for Security and Co-operation in Europe, Office for Democratic Institutions and Human Rights. (2023). *Handbook for the observation of election administration*. OSCE/ODIHR. https://odihr.osce.org/odihr/elections/544240

[68] Global Network for Securing Electoral Integrity. (2024). *Guidelines for safeguarding election management body independence in engagement with other public institutions*. GNSEI. https://www.ifes.org/news/global-network-securing-electoral-integrity

3. Ensure transparency in the election management body's decision-making during emergencies or extraordinary circumstances.

When emergency powers or crisis measures affect electoral processes, EMBs should document and publicly explain election-related decisions, including their legal basis, scope, and duration. EMBs should also clearly communicate the nature of their coordination with other public institutions and the limits of their authority.

This practice reflects OSCE principles of transparency and accountability in electoral administration, particularly in extraordinary circumstances, and is reinforced by GNSEI guidance highlighting transparency as essential to maintaining public trust and safeguarding EMBs' independence during crises.

4. Apply procedural safeguards to prevent politicized or discretionary enforcement.

Where EMBs are legally required to assess or refer alleged election-related violations, including those involving MDM, they should rely on clear, written procedures grounded in objective criteria and evidence. Any such actions should be narrowly confined to issues directly affecting election administration, with investigating and sanctioning authority exercised by courts or other competent bodies.

This approach is consistent with OSCE commitments on legality, due process, and proportionality in administrative decision-making and with GNSEI guidance cautioning against discretionary practices that could expose EMBs to political pressure or perceptions of bias.

5. Strengthen technical and analytical capacity while carefully considering enforcement roles.

EMBs should invest in internal capacity to analyze risks in the electoral information environment, including trends that could affect electoral operations or public confidence. Such capacity should inform communication strategies, risk assessments, and preparedness planning.

This recommendation aligns with OSCE principles of effectiveness and professionalism in election administration, as well as GNSEI guidance emphasizing capacity building as a means to reduce external reliance on external institutions and reinforce functional independence.

6. Align organizational structures with the election management body's neutral and impartial role.

Functions related to information integrity and public communication should be housed within nonenforcement units, such as voter education or communications departments. Internal policies and training should emphasize freedom of expression standards, proportionality, and the distinction between electoral administration and political debate.

This organizational approach reflects OSCE commitments to impartiality and GNSEI guidance recognizing institutional design as a key factor in shaping public perceptions of EMB independence.

7. Integrate information integrity and emergency-related risks into existing electoral risk frameworks.

Rather than creating new regulatory or enforcement mechanisms, EMBs should prioritize risks related to MDM in existing election integrity assessments and risk management tools. Mitigation strategies should focus on transparency, communication, coordination, and preparedness.

This approach is consistent with OSCE good practices on risk-based election planning and GNSEI guidance encouraging regular threat assessments as a means of safeguarding election integrity and EMB independence.

Appendix. Vulnerability map: risks to free expression during elections

This vulnerability map synthesizes risks that punitive misinformation, disinformation and malinformation (MDM) laws hold for democratic processes, including elections, drawing on comparative findings and international standards.

Key vulnerabilities

- **Overbroad countermeasures:** Broad or vague definitions of MDM enable discretionary enforcement and selective targeting of political opponents.
- **Institutional capture risks:** Election management bodies tasked with enforcement could be pressured to prioritize political objectives over impartial election administration. These risks are heightened when MDM frameworks are introduced without sufficient time, resources, or institutional preparedness.
- **Opaque enforcement:** Lack of transparency in takedown orders or sanctions reduces public trust in electoral institutions.
- **Judicial bottlenecks:** Courts face surges in politically sensitive cases with short timelines, reducing procedural safeguards.
- **Procedural deficits:** A lack of appeals or independent review leaves wronged parties without appropriate remedies. Legal reforms lack clarity and proportionality.

Consequences for the information environment

- **Chilling effects:** Fear of prosecution suppresses legitimate political discourse, especially online.
- **Media contraction:** Sanctions on journalists or outlets reduce the diversity of information available to voters.

References

Akua, N. (2025). *How Anti-Cybercrime Laws Are Being Weaponized to Repress Journalism*. *Columbia Journalism Review*. https://www.cjr.org/analysis/nigeria-pakistan-jordan-cybercrime-laws-journalism.php

Amnesty International. (2025, November). *Moldova: Fragile media challenged by vague laws, undue sanctions, and harassment*. https://www.amnesty.org/en/latest/news/2025/11/moldova-fragile-media-challenged-by-vague-laws-undue-sanctions-and-harassment

Amnesty International (2021). *Viet Nam: New leadership must seize opportunity to reverse human rights decline.* https://www.amnesty.org/en/latest/press-release/2021/01/viet-nam-new-leadership-reverse-human-rights-decline/

ANFREL (2025). *Interim Report: 2025 Philippine national and local midterm elections*. https://anfrel.org/interim-report-of-the-anfrel-ieom-to-the-2025-philippine-elections/

Article 19. (2023). *Social Media 4 Peace: A handbook to support freedom of expression*. https://www.article19.org/resources/social-media-4-peace-a-handbook-to-support-freedom-of-expression/

Baker McKenzie. (2024, October 4). Philippines: AI and social media guidelines for the 2025 elections issued by the COMELEC. InsightPlus. https://insightplus.bakermckenzie.com/bm/data-technology/philippines-ai-and-social-media-guidelines-for-the-2025-elections-issued-by-the-comelec

Barron, D. (2025). *Taiwan's model for digital defense of democracy goes global. The Diplomat*. https://thediplomat.com/2025/06/taiwans-model-for-digital-defense-of-democracy-goes-global/

BBC (2023). *Moldovan court bans pro-Russian party Sor.* *https://www.bbc.com/news/world-europe-65952878*

BBC (2020). *Maria Ressa: Philippine journalist found guilty of cyber libel*. https://www.bbc.com/news/world-asia-53046052

Brito, R., & Boadle, A. (2022, October 20). Brazil electoral court cracks down on disinformation ahead of Lula-Bolsonaro runoff. *Reuters*. *https://www.reuters.com/world/americas/brazil-electoral-court-cracks-down-disinformation-ahead-lula-bolsonaro-runoff-2022-10-20/*

Calvet-Bademunt, Jordi (2024). *The AI election panic: How fear-driven policies could limit free expression*. Tech Policy Press. https://www.techpolicy.press/the-ai-election-panic-how-feardriven-policies-could-limit-free-expression/

Carnegie Endowment for International Peace. (2024). *Countering disinformation effectively: An evidence-based policy guide*.

https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide

Center for Media, Data and Society. (2025). *Red-tagging in the Philippines: The modern McCarthyism threatening freedom of expression*. https://globalfreedomofexpression.columbia.edu/publications/red-tagging-in-the-philippines-the-modern-mccarthyism-threatening-freedom-of-expression

Carter Center. (2014). Election obligations and standards: A Carter Center assessment manual (2nd ed.). The Carter Center, https://www.cartercenter.org/wp-content/uploads/2025/08/cc-oes-handbook-10172014.pdf

Center for International Media Assistance (CIMA). (2023). *Chilling legislation: Tracking the impact of "fake news" laws on press freedom internationally* (G. Lim & S. Bradshaw). https://www.cima.ned.org/publication/chilling-legislation

CIVICUS. (2024). *Tanzania: End activist, media, and opposition crackdowns*. https://www.civicus.org/index.php/media-resources/news/7348-tanzania-end-activist-media-and-opposition-crackdowns

Cloudflare. (2025). *Helping protect the 2025 Moldova elections*. https://blog.cloudflare.com/helping-protect-the-2025-moldova-elections

CSO Meter. (2025). *Moldova: New proposal to impose fines for online disinformation*. https://csometer.info/updates/moldova-new-proposal-impose-fines-online-disinformation

CSO Meter. (2025). *Moldova 2024 country report*. https://csometer.info/countries/moldova

DFRLab. (2025, September 24). *Paid to post: Russia-linked digital army seeks to undermine Moldovan election*. https://dfrlab.org/2025/09/24/paid-to-post-russia-linked-digital-army-seeks-to-undermine-moldovan-election/

Digital Policy Alert. (2025). *Philippines: Implemented COMELEC guidelines on the use of social media, artificial intelligence and internet technology for the 2025 elections and the BARMM parliamentary elections*. https://digitalpolicyalert.org/event/23504-implemented-comelec-guidelines-on-the-use-of-social-media-artificial-intelligence-and-internet-technology-for-the-2025-elections-and-the-barmm-parliamentary-elections

Joan Donovan, PhD, Brian Friedberg, Gabrielle Lim, Nicole Leaver, Jennifer Nilsen, and Emily Dreyfuss (2021). "*Mitigating Medical Misinformation: A Whole-of-Society Approach to Countering Spam, Scams, and Hoaxes*," The Media Manipulation Casebook. https://mediamanipulation.org/research/mitigating-medical-misinformation-whole-society-approach-countering-spam-scams-and-hoaxes.

Egyptian Front for Human Rights (2024). *The path to the presidential palace: Monitoring and evaluation report of the Egyptian presidential elections 2023*. https://egyptianfront.org/2024/03/the-path-to-the-presidential-palace-monitoring-and-evaluation-report-of-the-egyptian-presidential-elections-2023/

Feldstein, S, (2025). *Digital Democracy in a Divided Global Landscape.* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/05/digital-democracy-in-a-divided-global-landscape?lang=en

Freedom House. (2024). *Freedom on the Net: Philippines*. https://freedomhouse.org/country/philippines/freedom-net/2024

Freedom House. (2024). *Freedom in the World: Moldova*. https://freedomhouse.org/country/moldova/freedom-world/2024

Global Network for Securing Electoral Integrity. (2024). *Guidelines for safeguarding election management body independence in engagement with other institutions*. https://www.ifes.org/news/global-network-securing-electoral-integrity

Global Network Initiative. (2025). GNI statement on Zambia's new cyber laws: A blow to freedom of expression and privacy. https://globalnetworkinitiative.org/gni-statement-on-zambias-new-cyber-laws-a-blow-to-freedom-of-expression-and-privacy/

IFES (2024). *Voluntary Election Integrity Guidelines for Technology Companies*. https://electionsandtech.org/election-integrity-guidelines-for-tech-companies/

Independent Journalism Center. (2025). *The media market in the Republic of Moldova: realities and trends in 2025*. https://cji.md/en/piata-mass-media-din-republica-moldova-realitati-si-tendinte-in-2025/

Information Technology and Innovation Foundation (2025). *Germany's Content Moderation Regulation*. https://itif.org/publications/2025/06/02/germany-content-moderation-regulation/

Inter-American Commission on Human Rights. (2022). *Pandemic and human rights: Report of the Inter-American Commission on Human Rights* (OEA/Ser.L/V/II. Doc. 396/22). Organization of American States. https://www.oas.org/en/iachr/reports/pdfs/2023/pandemiaddhh_en.pdf

IPI. (2025). *Moldova: Authorities issue takedown orders on 52 websites accused of spreading "fake news"*. https://ipi.media/alerts/moldova-authorities-issue-takedowns-orders-on-52-websites-accused-of-spreading-fake-news/

Khan, Irene. (2025). *A/HRC/59/50: Freedom of expression and elections in the digital age: Report of the Special Rapporteur*. OHCHR. https://docs.un.org/en/A/HRC/59/50

Mansour, S. (2018). Censorship tightens in Egypt as el-Sisi prepares for re-election bid. Committee to Protect Journalists. https://cpj.org/2018/03/censorship-tightens-in-egypt-as-el-sisi-prepares-f/

Masara, W. B. (2025). How Zambia's cyber laws rebrand repression. *Journal of Democracy*. https://www.journalofdemocracy.org/online-exclusive/how-zambias-cyber-laws-rebrand-repression/

Mozilla. (2022, April 5). *Philippines SIM card-registration act will expose users to greater privacy and security risks online*. https://blog.mozilla.org/netpolicy/2022/04/05/philippines-sim-card-registration-act-will-expose-users-to-greater-privacy-and-security-risks-online/

Organization for Security and Co-operation in Europe, Office for Democratic Institutions and Human Rights. (2023). *Handbook for the observation of election administration*. OSCE/ODIHR. https://odihr.osce.org/odihr/elections/544240

OSCE Office for Democratic Institutions and Human Rights. (2025, March 14). *Moldova: Presidential election and constitutional referendum 20 October and 3 November 2024 — Final report*. https://odihr.osce.org/odihr/elections/moldova/587451

Patal, Ajay (2025). Freedom of expression, artificial intelligence and elections. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000393473

Philippine News Agency. (2025, January 28). *Provisional authority for Starlink to bridge digital divide in PH*. https://www.pna.gov.ph/index.php/articles/1242786

Promo-LEX. (2025). *Massive online networks that manipulate voting*. https://promolex.md/en/massive-online-networks-that-manipulate-voting

Promo-LEX. (2025). *Election observation report No. 1*. https://promolex.md/en/report-no-1-observation-mission-for-the-parlamentary-elections-of-28-september-2025/

Rappler (2023). *Monkey's photo passes in SIM card registration in Philippines*. https://www.rappler.com/business/monkey-photo-register-sim-card-registration-philippines/

Sigla Research Center. (2025). *2025 Philippine elections report*. https://siglaresearch.org/news-and-events/2025-elections-report/

Simon, J., Lauría, A., & Flores, C. (2023). *Weaponizing the law: Attacks on media freedom*. Thomson Reuters Foundation. https://www.trust.org/wp-content/uploads/legacy/weaponizing-law-attacks-media-freedom-report-2023.pdf

Sobel, A. (2020). *The Philippines' Antiterror Bill Will Stifle Dissent. Carnegie Endowment for Democracy.* https://carnegieendowment.org/posts/2020/06/the-philippines-antiterror-bill-will-stifle-dissent?lang=en

Tapsell, R. (2021). *Social media and elections in Southeast Asia: The emergence of subversive, underground campaigning. information, digital media, and elections in Indonesia*. Asian Studies Review, 45(1), 117–134.

turn.io. (2023). *CNE launches "Vot-A" — WhatsApp chatbot for all voters*. https://www.turn.io/news/cne-vot-a-chatbot

Zamudio-Tordecilla, G. (2023, October 26). Nigeria, Pakistan, Jordan: How broadly written cybercrime laws threaten journalism. *Columbia Journalism Review*. https://www.cjr.org/analysis/nigeria-pakistan-jordan-cybercrime-laws-journalism.php

Ziarul de Gardă & BBC. (2025). *How Russian-funded fake news network aims to disrupt election in Europe - BBC investigation*. https://www.bbc.com/news/articles/c4g5kl0n5d2o

2000 M Street NW, Washington, DC, 20036, United States

www.IFES.org