



The Regulation of Digital Platforms in Mexico, Central America and the Caribbean

From Diagnosis based on the UNESCO Guidelines for the Governance of Digital Platforms to a Roadmap for Action

Rodrigo Cetina-Presuel, José Achoy, Priscilla Ruiz

Project supported by:



Funded by
the European Union



Barcelona 2026

Authors: Rodrigo Cetina-Presuel, José Achoy y Priscilla Ruiz

Collaborators: Daniel Nuñez, Andrés Rincón y Alberto Saldaña

For more information: rodrigo.cetina@bsm.upf.edu

Project Financed by the European Union: 'Safeguarding Freedom of Expression and Access to Information through the implementation of the UNESCO Guidelines for the Governance of Digital Platforms'

Project supported by:



Partners:



Table of Contents

TABLE OF CONTENTS.....	1
EXECUTIVE SUMMARY.....	4
1. INTRODUCTION.....	5
2. REGIONAL CONTEXT IN MEXICO, CENTRAL AMERICA, AND THE CARIBBEAN	8
2.1 INTERNATIONAL HUMAN RIGHTS FRAMEWORK.....	8
2.2 CONNECTIVITY AND INTERNET ACCESS IN THE REGION	10
2.3 FREEDOM OF EXPRESSION AND PLATFORM GOVERNANCE IN THE REGION	12
3. COUNTRY ANALYSIS: COSTA RICA.....	14
3.1 POLITICAL AND LEGAL SYSTEM	14
3.2 FREEDOM OF EXPRESSION AND HUMAN RIGHTS	14
3.3 DIGITAL ENVIRONMENT.....	16
3.4 DIGITAL PLATFORMS AVAILABLE IN THE COUNTRY.....	17
3.5 LEGISLATIVE AND REGULATORY CONTEXT IN COSTA RICA	18
3.5.1 <i>Constitutional Framework</i>	18
3.5.2 <i>Telecommunications and Media Legislation</i>	18
3.5.3 <i>Specific Regulations on Platforms and/or Content Regulation</i>	19
3.5.4 <i>Data Protection and Privacy Legislation</i>	20
3.5.5 <i>Specific Regulations on the Protection of Vulnerable Groups</i>	21
3.5.6 <i>Digital Election Regulations</i>	21
3.5.7 <i>The Digital Services and E-Commerce Governance Act (2026): A Regulatory Milestone</i>	22
3.6 ALIGNMENT WITH UNESCO GUIDELINES: COSTA RICA.....	23
4. COUNTRY ANALYSIS: EL SALVADOR	25
4.1 POLITICAL AND LEGAL SYSTEM	25
4.2 FREEDOM OF EXPRESSION AND HUMAN RIGHTS	26
4.4 DIGITAL PLATFORMS AVAILABLE IN THE COUNTRY.....	28
4.5 LEGISLATIVE AND REGULATORY CONTEXT IN EL SALVADOR	28
4.5.1 <i>Constitutional Framework</i>	28
4.5.2 <i>Telecommunications and Media Legislation</i>	29
4.5.3 <i>Specific Regulations on Platforms and/or Content Regulation</i>	30
4.5.4 <i>Data Protection and Privacy Legislation</i>	31
4.5.5 <i>Specific Regulations on the Protection of Vulnerable Groups</i>	32
4.5.6 <i>Digital Electoral Regulations</i>	33
4.6 ALIGNMENT WITH UNESCO GUIDELINES: EL SALVADOR	34
5. COUNTRY ANALYSIS: GUATEMALA	35
5.1 POLITICAL AND LEGAL SYSTEM	35
5.2 FREEDOM OF EXPRESSION AND HUMAN RIGHTS	35
5.3 DIGITAL ENVIRONMENT.....	38
5.4 DIGITAL PLATFORMS AVAILABLE IN THE COUNTRY.....	39
5.5 LEGISLATIVE AND REGULATORY CONTEXT IN GUATEMALA	40
5.5.1 <i>Constitutional Framework</i>	40
5.5.2 <i>Telecommunications and Media Legislation</i>	41
5.5.3 <i>Specific Regulations on Platforms and/or Content Regulation</i>	41
5.5.4 <i>Data Protection and Privacy Legislation</i>	42
5.5.5 <i>Specific Regulations on the Protection of Vulnerable Groups</i>	42
5.6 ALIGNMENT WITH UNESCO GUIDELINES: GUATEMALA	43
6. COUNTRY ANALYSIS: HONDURAS	45

6.1 POLITICAL AND LEGAL SYSTEM	45
6.2 FREEDOM OF EXPRESSION AND HUMAN RIGHTS	45
6.3 DIGITAL ENVIRONMENT.....	47
6.4 DIGITAL PLATFORMS AVAILABLE IN THE COUNTRY.....	47
6.5 LEGISLATIVE AND REGULATORY CONTEXT IN HONDURAS.....	48
6.5.1 <i>Constitutional Framework</i>	48
6.5.2 <i>Telecommunications and Media Legislation</i>	48
6.5.3 <i>Specific Regulations on Platforms and/or Content Regulation</i>	49
6.5.4 <i>Legislation on data protection and privacy</i>	50
6.5.5 <i>Specific Regulations on the Protection of Vulnerable Groups</i>	50
6.6 ALIGNMENT WITH UNESCO GUIDELINES: HONDURAS	51
7. COUNTRY ANALYSIS: MEXICO	53
7.1 POLITICAL AND LEGAL SYSTEM	53
7.2 FREEDOM OF EXPRESSION AND HUMAN RIGHTS	55
7.3 DIGITAL ENVIRONMENT.....	58
7.4 DIGITAL PLATFORMS AVAILABLE IN THE COUNTRY.....	59
7.5 LEGISLATIVE AND REGULATORY CONTEXT IN MEXICO	60
7.5.1 <i>Constitutional Framework</i>	60
7.5.2 <i>Telecommunications and Media Legislation</i>	61
7.5.3 <i>Specific Regulations on Platforms and/or Content Regulation</i>	62
7.5.4 <i>Data Protection and Privacy Legislation</i>	65
7.5.5 <i>Specific Regulations on the Protection of Vulnerable Groups</i>	67
7.5.6 <i>Digital Electoral Regulation</i>	68
7.6 ALIGNMENT WITH UNESCO GUIDELINES: MEXICO	69
8. COUNTRY ANALYSIS: PANAMA	71
8.1 POLITICAL AND LEGAL SYSTEM	71
8.2 FREEDOM OF EXPRESSION AND HUMAN RIGHTS	72
8.3 DIGITAL ENVIRONMENT.....	74
8.4 DIGITAL PLATFORMS AVAILABLE IN THE COUNTRY.....	75
8.5 LEGISLATIVE AND REGULATORY CONTEXT IN PANAMA.....	75
8.5.1 <i>Constitutional Framework</i>	76
8.5.2 <i>Telecommunications and Media Legislation</i>	76
8.5.3 <i>Specific Regulations on Platforms and/or Content Regulation</i>	78
8.5.4 <i>Data Protection and Privacy Legislation</i>	80
8.5.5 <i>Specific Regulations on the Protection of Vulnerable Groups</i>	81
8.5.6 <i>Digital Election Regulations</i>	82
9. COUNTRY ANALYSIS: DOMINICAN REPUBLIC	85
9.1 POLITICAL AND LEGAL SYSTEM	85
9.2 FREEDOM OF EXPRESSION AND HUMAN RIGHTS	85
9.3 DIGITAL ENVIRONMENT.....	87
9.4 DIGITAL PLATFORMS AVAILABLE IN THE COUNTRY.....	88
9.5 LEGISLATIVE AND REGULATORY CONTEXT IN THE DOMINICAN REPUBLIC	88
9.5.1 <i>Constitutional Framework</i>	88
9.5.2 <i>Telecommunications and Media Legislation</i>	89
9.5.3 <i>Specific Regulations on Platforms and/or Content Regulation</i>	91
9.5.4 <i>Data Protection and Privacy Legislation</i>	93
9.5.5 <i>Specific Regulations on the Protection of Vulnerable Groups</i>	94
9.5.6 <i>Digital Electoral Regulations</i>	95
9.6 ALIGNMENT WITH UNESCO GUIDELINES: DOMINICAN REPUBLIC.....	96
10. ALIGNMENT WITH UNESCO GUIDELINES FROM A REGIONAL PERSPECTIVE.....	98
11. TRAINING WORKSHOPS FOR MEXICO, CENTRAL AMERICA, AND THE CARIBBEAN	101
11.1 KEY CONTRIBUTIONS AND CONCLUSIONS FROM THE WORKSHOPS	101
11.2 ANALYSIS OF THE MAIN REGIONAL CHALLENGES AND PRIORITIES	105

12.	CONCLUSIONS AND RECOMMENDED ACTIONS	109
12.1	KEY CONCLUSIONS	109
12.2	RECOMMENDED ACTIONS	110
13.	BIBLIOGRAPHY	112

Executive Summary

The primary objective of this report is to map and analyze the existing legal and regulatory framework in seven Spanish-speaking countries in Central America and the Caribbean (Costa Rica, El Salvador, Guatemala, Honduras, Mexico, Panama, and the Dominican Republic) regarding the governance of digital platforms. Through this assessment, the report evaluates the extent to which national regulations align with the principles and recommendations of **UNESCO's Guidelines for the Governance of Digital Platforms**, with the aim of identifying gaps, challenges, and opportunities for building an ethical, inclusive digital ecosystem that respects human rights.

The analysis reveals a profound dichotomy in the region: while all seven countries have a robust constitutional framework that protects freedom of expression, prohibits prior censorship, and enshrines the privacy of communications, the operational and regulatory reality presents critical gaps. Most of the states analyzed lack a comprehensive legal framework regulating intermediaries and robust personal data protection laws applicable to the private sector (with the exception of Mexico and Panama). Faced with this gap, authorities often resort to sector-specific, reactive, and frequently punitive approaches (such as applying criminal laws designed for traditional contexts to digital environments), moving away from the model of shared responsibility and proactive transparency promoted by UNESCO.

Furthermore, the region's institutional design shows deficiencies regarding the autonomy of regulators. The agencies in charge are often subordinate to the executive branch. This situation is exacerbated by recent setbacks, such as the dissolution of autonomous transparency and telecommunications bodies in Mexico, or the existence of states of emergency and state surveillance regimes in El Salvador, which have a chilling effect on civic space and journalism.

In the electoral sphere, the rise of social media, microsegmentation, and generative Artificial Intelligence (AI) has outpaced the technical and legal capacities of most electoral courts, leaving the region's democracy highly vulnerable to disinformation. A notable positive exception is Panama, a pioneer in criminalizing mass manipulation through *bots* and *deepfakes*.

To validate these findings and chart a roadmap, training and co-creation workshops were held on December 8 and 9, 2025, in Santo Domingo, Dominican Republic, led by the I4T Knowledge Network and UNESCO, under a multi-stakeholder approach. These workshops brought together electoral authorities and regulatory bodies from all countries covered by the report (except Guatemala, which was unable to participate) as well as regional and national civil society organizations.

These dialogues yielded clear strategic priorities that serve to chart a roadmap for the coming years: the need to shift from content moderation to the regulation of processes and algorithms; the urgency of demanding "linguistic sovereignty" that requires platforms to moderate content while respecting local idioms and indigenous languages; and the innovative proposal to use banking and tax authorities to exert coercive pressure on technology corporations ("follow the money").

Finally, it was concluded that countries in the region lack the individual market clout to negotiate with *Big Tech*, making it imperative to create a unified regional bloc to demand accountability and protect human rights in the digital ecosystem.

1. Introduction

The main objective of this report is to map and analyze the existing legal and regulatory framework in several Spanish-speaking countries in the Central American and Caribbean region, with an emphasis on Mexico, Guatemala, Honduras, El Salvador, Costa Rica, Panama, and the Dominican Republic. The aim is that, by identifying applicable regulations, it will be possible to assess the alignment of national policies and regulations with the fundamental principles and recommendations contained in UNESCO's Guidelines for the Governance of Digital Platforms, serving as a preliminary assessment to open a dialogue in the region and identify priorities and the way forward.

In this context, the analysis focuses on identifying the legal frameworks governing the operation of digital platforms, including regulations on data protection, fundamental rights, telecommunications, transparency, and the handling of disinformation in election campaigns. It will also be important to identify the bodies, agencies, or institutions responsible for overseeing and safeguarding these rights, guarantees, and freedoms.

The report aims not only to map existing regulations but also to assess potential regulatory gaps and challenges that persist in the region, as well as opportunities for improvement to foster a digital ecosystem that is more inclusive, ethical, and in line with international standards regarding the governance of digital platforms. All of this is done while highlighting the differences and unique contexts of each country in the region.

Methodologically, an analysis of the legal and regulatory framework was conducted using normative legal sources for each country in question, also compiling relevant information such as the year of enactment, the bodies that issued these regulations, their scope, and their areas of application, among other details. This review included constitutional, statutory, and regulatory texts, as well as other lower-level regulations issued by institutional agencies in the countries of the region that are related to or pertain to digital platforms.

This comprehensive approach sought to provide a complete overview of the regulatory framework governing digital governance in the various national contexts. Where necessary, data was also collected and reports were cited that assess particularly relevant issues, such as the state of freedom of expression or freedom of the press in the region, and the democratic challenges facing these countries.

The analysis was structured around the fundamental principles set forth in UNESCO's Guidelines for the Governance of Digital Platforms, which serve as a reference framework for assessing the consistency and alignment of national regulations with international standards regarding the governance of digital platforms. Although there is no direct evidence that the UNESCO Guidelines have influenced recent regulatory changes—particularly since, in several cases, no such changes have occurred—the report uses the Guidelines as a starting point to identify areas where existing policies and regulations align with these principles, as well as those where there are divergences, regulatory gaps, or even tensions; or, failing that, areas where regulation does not yet exist.

Based on this, a country-by-country assessment was conducted to determine, *a priori*, the extent to which each country's legal framework aligns with the content of the Guidelines. The assessment also examined the degree of compliance and effectiveness in safeguarding these aspects by the responsible bodies. The approach is geared toward identifying regulatory patterns, regulatory gaps, and areas of opportunity, which enriches the comparative assessment and the formulation of recommendations.

Overall, the review of regulatory documents seeks to contribute to a deeper understanding of the challenges and opportunities for improving digital governance in the region, in line with the principles promoted by UNESCO. This is achieved by analyzing the general Central American context of this issue as a whole, while highlighting the specific national characteristics.

All of this led to the convening, on December 8 and 9, 2025, with support from UNESCO, the I4T Knowledge Network—in collaboration with the UPF Barcelona School of Management and a number of researchers and specialists—of representatives from regulatory and electoral bodies, as well as representatives from civil society organizations, for a series of training workshops, active listening sessions, and creative sessions. The aim was to present the findings of this report and supplement them with a series of activities designed not only to validate the report but also to provide an assessment of regional and national challenges regarding the governance of digital platforms. This, in turn, would enable the identification of a set of proposals and priorities for directing these efforts in the region.

These workshops took place in Santo Domingo, Dominican Republic, in a hybrid format (in-person and *online*). This event was part of the UNESCO project titled “*Safeguarding Freedom of Expression and Access to Information through the Implementation of the UNESCO Guidelines for the Governance of Digital Platforms*,” which, like this report, is funded and supported by the European Union.

To ensure a free and open environment for debate, the sessions were conducted under the *Chatham House Rule*, allowing participants to use the information shared without revealing the identity or affiliation of the speakers. The event was organized through a broad inter-institutional and academic partnership. Among the organizing and collaborating entities were higher education institutions and global networks, such as the UPF Barcelona School of Management, which led the organization and delivery of the workshops; the Complutense University of Madrid; the Catholic University of Santo Domingo (UCSD), which served as the local organizer; the Global Network for Electoral Justice; and the Institute for Training and Studies in Democracy (IFED) of the Supreme Electoral Tribunal of Costa Rica.

All of this was carried out within a framework of prior awareness-raising regarding the UNESCO Guidelines among those present, so that they could serve as a conduit to the entities they represent and so that, using the Guidelines themselves as a context, any proposals and priorities established would seek to align with their framework and with the goal of providing robust protection for human rights in the context of private platform governance, which has significant implications for freedom of expression, freedom of the press, political participation, and other important personal rights such as non-discrimination, the protection of physical and mental well-being, and the protection of privacy and personal data, among others.

Among the outcomes of these workshops, which are included in the final section of this report, the Periodic Table of Platform Regulation, created by the I4T Knowledge Network, was an essential tool. The table is a visual tool that organizes the key elements of digital platform governance. It is inspired by the periodic table of chemical elements and facilitates the exploration and understanding of the different dimensions of digital platform regulation.

Although the original version of the Table is used to collect examples of digital platform regulation and governance practices—in order to systematize them and provide elements for their analysis and evaluation—a modified version was used in the workshops to apply a co-creation methodology that allowed for the systematic collection of participants’ contributions regarding potential regulatory or digital governance initiatives.

The contributions were based on reflections regarding the necessary institutional framework, the authorities that should be involved and their powers, the types of legislative mechanisms that exist or are lacking, the human rights that the interventions seek to protect, and, in a second part, the types of interventions—content governance, risk management and due diligence obligations, and technological and prosocial design interventions—that can be used for the governance and regulation

of digital platforms. All of this enabled participants to use this framework—based on the UNESCO Guidelines—to self-assess their national situations, make proposals, and compare them with the ideas and proposals from other participating countries, thereby identifying joint priorities and needs specific to local and regional contexts.

2. Regional Context in Mexico, Central America, and the Caribbean

2.1 International Human Rights Framework

The countries targeted by our study are part of the Inter-American System for the Protection of Human Rights (SIDH). In this context, they are signatories to the American Convention on Human Rights (Pact of San José, hereinafter ACHR)¹ and to other instruments that broaden the substantive scope of fundamental rights, such as the International Covenant on Civil and Political Rights (ICCPR) or the International Covenant on Economic, Social, and Cultural Rights (ICESCR). Of particular interest to this study, the ICESCR, as an international legal instrument, has been instrumental in promoting democratization in access to information and the use of information and communication technologies for the region's inhabitants. The latter is in accordance with Article 13 of the American Convention on Human Rights (ACHR), which establishes the right to freedom of thought and expression, implying the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers and by any means.

The Inter-American Court of Human Rights (IACHR) has also played a central role in defining the substantive and procedural scope of the protection of these freedoms and rights. In Advisory Opinion OC-5/85 of 1985, it was established for the first time that freedom of expression includes the right to seek and receive information, which laid the groundwork for the subsequent development of access to information as an autonomous right within the inter-American system². In 2006, the IACHR defined the scope of the right of access to information, with special emphasis on the positive obligations that States have to guarantee it, and which confer upon them the mandate in these areas.

In the cases of *Bronstein v. Peru*³ and *Herrera Ulloa v. Costa Rica*⁴, the IACHR weighed the scope of freedom of expression, as well as access to information and the role of the media—principles that can now be extrapolated to digital ecosystems through which interactions occur and information flows for the benefit of society and individuals.⁵

With regard to these rights and freedoms, the region summarizes their context as follows: a) the constitutional enshrinement and protection of access to information in the late 20th and early 21st centuries; b) an assessment of the scope, boundaries, and limitations of freedom of information and expression; and c) the extra-legal challenges related to the provision and guarantee of these freedoms and rights, primarily due to issues of the digital divide (protection of the right to telecommunications) and the authoritarian exercise of power.

¹American Convention on Human Rights, November 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123.

²Inter-American Court of Human Rights. (November 13, 1985). *Mandatory membership in a professional association for journalists (Arts. 13 and 29 of the American Convention on Human Rights)* (Advisory Opinion OC-5/85, Series A No. 5). <https://www.corteidh.or.cr/tablas/a12040.pdf>

³Inter-American Court of Human Rights. (February 6, 2001). *Case of Ivcher Bronstein v. Peru* (Judgment on the merits, reparations, and costs, Series C No. 74). https://www.corteidh.or.cr/docs/casos/articulos/seriec_74_esp.pdf

⁴Inter-American Court of Human Rights. (July 2, 2004). *Case of Herrera Ulloa v. Costa Rica* (Judgment on Preliminary Objections, Merits, Reparations, and Costs, Series C No. 107). <https://hrlibrary.umn.edu/iachr/C/107-esp.html>

⁵The following cases may also be taken into consideration: *Gerardi v. Guatemala* (1982); *Estiverne v. Haiti* (1988); *Verbitsky v. the State of Argentina* (1994); “The Last Temptation of Christ” Case: *Olmedo Bustos et al. v. Chile* (2001); *Ricardo Canese v. Paraguay* (2004); *Palamara Iribarne v. Chile* (2005).

In this regard, the concept of a constitutional heritage in Central America and the Caribbean has recognized that, when it comes to constitutional norms and history,⁶ the countries in this region have more common ground than differences. This has meant that, in the case of rights such as access to information and telecommunications, as well as freedom of expression and the processes for their recognition and protection, these rights have also evolved through similar periods and movements.

However, not everyone experiences the same reality when it comes to freedom of access to information and the free expression of ideas on digital platforms. This, clearly, creates contrasts that go beyond normative ideals and call into question the effectiveness of these fundamental guarantees for daily life in a democracy.

As explained earlier, these are elements that form part of the body of conventions to which the States of the Inter-American region are bound. In fact, Inter-American case law has established the obligation of countries in this area to bring their domestic legal systems into line with international standards regarding access to information, based on the following fundamental premises: (i) removing legal or administrative obstacles that hinder access to information; (ii) promoting the implementation of the right of access within all relevant entities and authorities—through the adoption and enforcement of regulations, procedures, and training for authorities regarding the custody, administration, archiving, and provision of information; and (iii) in general terms, adopting a public policy conducive to the full exercise of this right. Indeed, as the Inter-American Court has explained, States must have an adequate legal framework for the protection of the right of access to information and must ensure the effectiveness of an appropriate administrative procedure for processing and resolving requests for information, with clear deadlines for resolving such requests and providing the information, under the supervision of officials duly trained in this area (...).⁷

This is integral to freedom of expression as a fundamental guarantee of democracy and within a human rights framework. In this regard, the Court has established the significance of this freedom for the legal systems and political structures of the continent: Freedom of expression is a fundamental element upon which the existence of a democratic society is based. It is indispensable for the formation of public opinion. It is also a *conditio sine qua non* for political parties, labor unions, scientific and cultural societies, and, in general, those who wish to influence the community to develop fully. It is, in short, a prerequisite for the community to be sufficiently informed when exercising its choices. Therefore, it can be asserted that a society that is not well-informed is not fully free.⁸

The conditions and possibilities associated with freedom of information are thus linked to the reality of fundamental rights and democracy. In summary, the Court's rulings have established that these rights are not only individual guarantees but also essential conditions for informed citizen participation and the full exercise of other political and social rights. Thus, the effective protection of these freedoms requires specific actions on the part of States, but these must be in accordance with international standards.

Although this is a phenomenon composed of multiple factors, this study focuses on the regulatory conditions governing digital platforms in the selected Spanish-speaking countries of Central America and the Caribbean. Specifically, the study examines their development and operation, as well as the impact this has on guarantees and freedoms of information for their citizens, and compares this with the human rights protections that the UNESCO Guidelines for the Governance of Digital Platforms seek to promote.

⁶Ulate Chacón, E. N. (2015). *From Central American Constitutional Heritage to Central American Constitutional Law: Studies in Comparative Law*. ISOLMA.

⁷Inter-American Court of Human Rights. (September 19, 2006). *Case of Claude Reyes et al. v. Chile* (Judgment on the Merits, Reparations, and Costs, Series C No. 151). https://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf

⁸Inter-American Court of Human Rights. (August 31, 2004). *Case of Ricardo Canese v. Paraguay* (Judgment on the Merits, Reparations, and Costs, Series C No. 111). https://www.corteidh.or.cr/docs/casos/articulos/seriec_111_esp.pdf

Various reports have generally pointed out that Latin America lacks adequate regulation to protect the relationships between users and digital platforms, as well as their operation and scope⁹. Case law and specific studies indicate that some states still face difficulties in guaranteeing even the most basic aspects of these rights.

This could be linked to government restrictions on service provision or, failing that, to democratic backsliding that jeopardizes access to information¹⁰. In other words, this is a regional context marked by legal tensions regarding the recognition and protection of rights and freedoms in these types of digital information ecosystems. Numerous reports have previously addressed the crisis facing some Central American countries regarding these rights and freedoms.¹¹

2.2 Connectivity and Internet Access in the Region

Some general data provide context for understanding this reality, although it should not be overlooked that the region also faces challenges regarding internet availability and accessibility. Several studies have gathered information on the status of certain indicators related to this issue.

One of the first examples involves the available data on the number of internet users relative to the population by country: Costa Rica, the Dominican Republic, and Mexico are above the Latin American average. However, the rest of the Central American countries appear to have a lower number of users compared to the Latin American average.

The literature has repeatedly emphasized the importance of internet access and use as a source of information, especially in the context of digital ecosystems¹². In fact, in countries such as Costa Rica, internet access is a human right that can be enforced before the Constitutional Court.¹³

Although a lower number of users would not necessarily indicate an uninformed society, countries with lower scores on this index may face challenges in ensuring access to communication networks and platforms, as well as obstacles to developing digital and information literacy for the benefit of their citizens.

⁹ Other challenges stem from the authoritarian exercise of power in some countries, which erodes democratic debate, hinders the full exercise of freedom of expression, and restricts the free flow of information. For more on this, see the reports of the Program on Freedom of Expression and the Right to Information, such as: Program on Freedom of Expression, the Right to Information, and Public Opinion. (n.d.). PROLEDI Publications. University of Costa Rica. Retrieved March 3, 2026, from <https://proledi.ucr.ac.cr/publicaciones-proledi/>

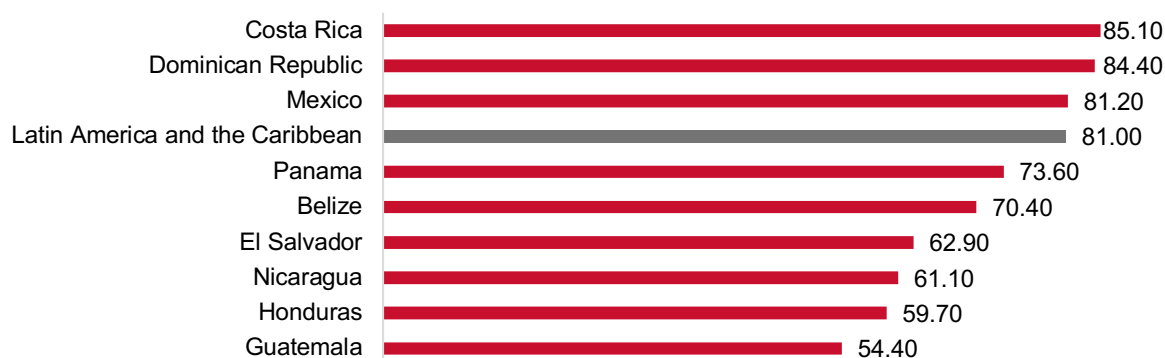
¹⁰ Center for Transdisciplinary Studies in Central America. (September 27, 2023). *Authoritarianism in Central America: Unlawful Criminal Prosecution in Guatemala, El Salvador, Honduras, and Nicaragua*. <https://www.cetcam.org/los-autoritarismos-en-centroamerica-promueven-la-persecucion-penal-ilegitima/>

¹¹ In this regard, see the special reports issued by the Special Rapporteur for Freedom of Expression of the Organization of American States regarding access to information (Special Rapporteur for Freedom of Expression. (n.d.). Access to Information. Inter-American Commission on Human Rights. Retrieved March 3, 2026, from https://www.oas.org/es/cidh/expresion/temas/acceso_informacion.asp and on freedom of expression (UNESCO. (September 28, 2024). Transparency and Access to Public Information in Latin America and the Caribbean: Pillars of Democracy. <https://www.unesco.org/es/articles/la-transparencia-y-el-acceso-la-informacion-publica-en-america-latina-y-el-caribe-pilares-de-la-expresion>).

¹² In this regard, see sources such as: Mondragón Toledo, G. (2015). The Importance of the Internet as a Source of Power for Society. *Digitum*, University of Murcia; Cebrián Zazurca, E. (2016). The Impact of the Internet on the Democratic State. *Journal of Political Studies*, (173), 307–320; Mindus, P. (2014). What Does “E-” Add to Democracy?: Designing an Agenda for Democracy Theory in the Information Age. In J. Bishop (Ed.), *Transforming Politics and Policy in the Digital Age*.

¹³ Since 2012, the Constitutional Chamber of the Supreme Court of Justice has ruled that Internet access is protected by the right to freedom of expression and communication, establishing it as an essential right for the exercise of other civil and political rights (rulings nos. 2012-15018, 2014-0531, and 2016-10997).

Figure 1. Percentage of internet users relative to the total population in Central American countries, 2023.



Source: Ritchie, H., Mathieu, E., Roser, M., & Ortiz-Ospina, E. (2023). *Internet*. Our World in Data. <https://ourworldindata.org/internet>

According to the report **Digital 2025: Global Overview Report** prepared by Simon Kenp of DataReportal, on average, 66.6% of the total population in Central America uses digital platforms, representing 84.1% of the region's internet users.¹⁴

For its part, since 2020, Latinobarómetro has included a variable to gauge public perception regarding the use of social media and digital platforms in the political context. The study's results show similarities among countries with different political regimes. For example, in Costa Rica (full democracy) and Nicaragua (authoritarian regime), nearly half of those surveyed indicated that social media is not useful for participating in politics.

Although these are societies and political contexts with divergent circumstances, their populations share a similar perception of the use of digital platforms for these purposes. In contrast, the Dominican Republic (40.4%), El Salvador (30.7%), Guatemala (20.2%), and Mexico (19.6%) show a public perception that is more favorable toward the compatibility of social media with its use for political participation.

Table 1: Percentage of public perception regarding the use of social media in politics, by country. 2020.

Which of these statements do you agree with?	CRC	DOM	SLV	GUA	MEX	NIC	PAN
Social media allows people to participate in politics.	17.4	40.4	30.7	20.2	19.6	15.6	17.0
Social media creates the illusion that one is participating in politics.	24.8	17.1	22.1	15.2	24.8	9.8	22.1
Social media is not useful for participating in politics.	49.3	30.0	32.8	37.1	36.2	51.4	44.8
Don't know.	7.3	10.1	11.1	23.6	18.2	18.6	13.8

Source: Latinobarómetro Corporation. (2020). *2020 Report*. <https://www.latinobarometro.org/latOnline.jsp>

In that same study, people were asked about the medium through which they primarily express their opinions on the country's problems. In 2020, 8.4% of respondents indicated that social media was the

¹⁴DataReportal. (n.d.). *DataReportal: Global digital insights*. Retrieved August 27, 2025, from <https://datareportal.com/>

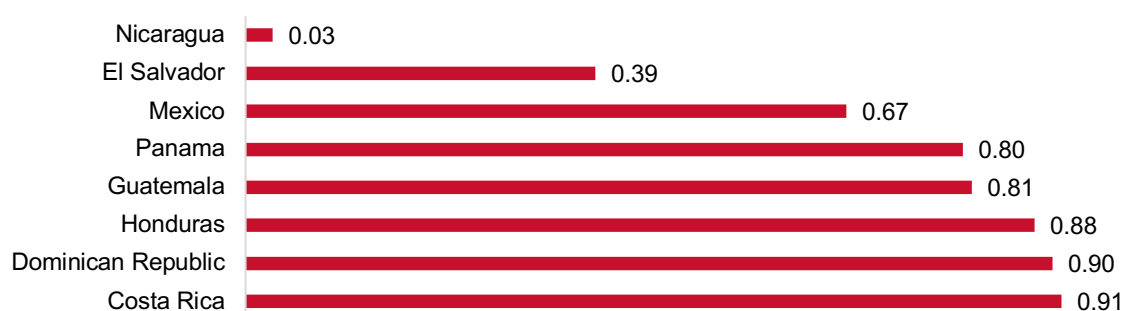
space where they addressed these issues. At that time, digital platforms ranked last among the various possible categories. However, by 2024, that figure had risen to 9.9%, and social media had overtaken social mobilization and collective action.¹⁵

2.3 Freedom of Expression and Platform Governance in the Region

When it comes to freedom of expression, countries also exhibit disparities. To measure this indicator, we use the Varieties of Democracy database (commonly known as V-Dem) and the visualizations processed by the University of Oxford on Our World in Data.

These are expert estimates of the extent of freedom of expression and of the press, measured on a scale from 0 (lowest) to 1 (highest). Societies in the countries of the region interact on digital platforms to express themselves, influence politics, and generate collective debate; but social media also reflects the freedoms inherent to democracy according to their particular contexts.

Figure 2. Freedom of Expression Index in Central American Countries, 2024.



Source: V-Dem (2025) – processed by Our World in Data. “Freedom of expression index – V-Dem” [dataset].¹⁶

UNESCO’s Guidelines for the Governance of Digital Platforms have as their central objective the safeguarding of freedom of expression, access to information, and other human rights in the regulation of digital platforms. To achieve this, they propose a governance system with a *multistakeholder* approach that respects human rights and promotes content moderation and curation processes based on risk mitigation.

By outlining the responsibilities of states, digital platforms, intergovernmental organizations, and civil society, these guidelines can serve as an essential standard or benchmark for analyzing the state of digital platform regulation in the Central American and Caribbean region. Specifically, they serve as a valuable resource for policymakers and regulatory bodies in the region to identify legitimate objectives and evaluate policies, and for civil society to advocate for regulation that protects human rights in the face of the challenges posed by the digital ecosystem.

Regarding the governance of digital platforms and the advancement of freedom of information in digital spaces across the region, the Guidelines clearly prioritize a human rights-based approach and a people-centered model. **The Spanish-speaking countries of Central America and the Caribbean covered in this report present contrasting realities—not only in terms of connectivity, usability, and access, but also regarding the characteristics of the legal frameworks and political systems that shape these conditions.**

¹⁵ Latinobarómetro Corporation. (2020). *2020 Report*. <https://www.latinobarometro.org/latOnline.jsp>

¹⁶V-Dem. (2025). Freedom of Expression Index - V-Dem [Dataset]. Our World in Data. <https://archive.ourworldindata.org/20250825-143526/grapher/freedom-of-expression-index.html>

Therefore, regulatory approaches require an understanding of the dynamics, challenges, and unique characteristics of the region and its inhabitants. For example, in this area, another challenge is digital autonomy or sovereignty and the regulatory measures needed to ensure it.

A recent UNDP publication revealed that Latin America and the Caribbean host only 4.8% of global data centers and infrastructure; of that percentage, Central America accounts for just 5%¹⁷. In other words, Latin American countries lack sufficient autonomy to host the data and information of users residing in the region. This situation is exacerbated in the case of Central Americans, as the isthmus is home to a very small portion of this infrastructure, which is vital for ensuring minimum safeguards in the processing of information and the hosting of data on digital platforms.

In summary, the region operates within a context where a framework of fundamental rights associated with freedom of information and freedom of expression is protected at the conventional level, along with the guarantees and obligations that states must fulfill to ensure that access to these platforms is a reality in citizens' daily lives.

Recognition within the framework of international conventions dates back many years, but its implementation at the national level and its adaptation to contemporary realities require evaluation. This study will delve into the regulatory landscape of Central American countries with regard to citizens' guarantees and freedoms on digital platforms, the development of independent authorities, and the information ecosystems that foster harmony between their operation and the full exercise of human rights. It will also be of primary interest to examine the role the State plays in providing its citizens and platforms with substantive and procedural provisions and ensuring their alignment with a fundamental rights-based approach.

¹⁷United Nations Development Programme. (2025, April 15). *Data in the Cloud, Centers on the Ground: The Role of Data Centers in the Digital Future of Latin America and the Caribbean*. <https://www.undp.org/es/latin-america/blog/datos-en-la-nube-centros-en-la-tierra-el-rol-de-los-centros-de-datos-en-el-futuro-digital-de-alc>

3. Country Analysis: Costa Rica

3.1 Political and Legal System

Costa Rica has a presidential system of government, and legislative proposals may be introduced by either the legislature or the executive branch. Within the Central American region, it has been characterized by high levels of democratic quality, and although it has experienced declines in recent years on The Economist's *Democracy Index*, it remains classified as a full democracy.

The political system is structured around the three branches of government (Executive, Legislative, and Judicial) and a Supreme Electoral Tribunal, which holds the same constitutional status. The country has held free and consecutive national elections since 1953, and currently, elections are held every four years to choose executive and legislative officials, with a midterm election for popularly elected local government officials, who are also appointed for four-year terms.

Costa Rica has a centralized system of constitutional review, and the Supreme Electoral Tribunal is granted exclusive and exhaustive authority to interpret the Constitution in electoral matters. This body has a dual function: it serves as both the electoral administration and the civil registry; additionally, it holds constitutional powers of judicial authority to protect political rights.

The organization of the State, in addition to the powers of these branches, is decentralized at the institutional level among ministries, autonomous, and semi-autonomous institutions; and, separately, through territorial decentralization into 7 provinces comprising 84 municipalities, each consisting of a mayor's office and a municipal council.

3.2 Freedom of Expression and Human Rights

Freedom of expression (Article 29), the right of access to information (Article 27), and the right to telecommunications (Article 24) are provisions expressly established in the Constitution and elaborated upon in case law by the Constitutional Chamber of the Supreme Court of Justice.

The country ranks as one of the main destinations for exiled Central American and Latin American journalists¹⁸, although the latest report from the OAS Special Rapporteur on Freedom of Expression warned of difficulties that have recently worsened for these individuals, primarily due to the cost of living and public insecurity, which has led them to pursue careers in other professional fields. The rankings and results in freedom of expression indices and reports for this country are as follows:

Table 2. Country Rankings in Freedom of Expression Indices

Index / Report	Rating	Rank	Year
Reporters Without Borders (RSF)	73.09	36	2025
V-Dem	0.94	23	2024

¹⁸University of Costa Rica. (2025). *Report on Displaced Voices*. <https://www.ucr.ac.cr/medios/documentos/2025/informe-voces-desplazadas-proledi-ucr-6882ccd979021.pdf>

Index / Report	Rating	Rank	Year
Freedom on the Net	85 (Free)	5(72)	2023

Source: Compiled by the author based on RSF (2025), V-Dem (2024), and Freedom House (2023).

Judicial protection of both freedom of and access to information and freedom of expression falls under the jurisdiction of the Constitutional Chamber through the amparo proceeding; and, with regard to these same freedoms in the context of election campaigns, the exercise of political rights, and grievances against elected officials, such cases are processed as amparo proceedings before the Supreme Electoral Tribunal.

In addition, the country has three administrative agencies involved in this area. The first of these is the Agency for the Protection of Residents' Data, which handles administrative complaints regarding the misuse of data, images, or personal information. This office also processes requests related to the "right to be forgotten" from individuals seeking the removal of news articles or digital content that is more than 10 years old and not in the public interest.

The second relevant institution is the Office of Advertising Control, whose jurisdiction is limited to regulating advertising (not editorial content) that involves the improper, violent, or inappropriate use of the image of women and older adults, as well as setting permitted time slots for television content.

The Superintendency of Telecommunications serves as a technical and administrative agency regarding regulations associated with the provision of public services, infrastructure, and the deployment of communication networks and the use of the radio spectrum. Primarily, it is responsible for regulating and supervising competition rules among private entities granted concessions for the use of the telecommunications spectrum.

Although it is not an administrative agency exclusively focused on the governance of digital platforms, it was determined that the General Directorate of Taxation, under the Ministry of Finance, plays an important role in this area. Following a 2018 tax reform, the State was legally authorized to levy a 13% Value-Added Tax on cross-border digital services. The list of platforms subject to this tax is not exhaustive by law; this delegates the authority to the General Directorate of Taxation to establish its criteria, include and exclude platforms through administrative resolutions, and set the procedure for collecting the tax.

According to the Constitutional Chamber's official records, in 2024, 41 amparo proceedings were filed alleging violations of freedom of expression and freedom of the press; additionally, 3,130 appeals were filed regarding the right to petition and access to information. Collectively, these proceedings accounted for 8% of the cases processed by the Constitutional Court during that year.¹⁹ 49% of those cases were upheld in full or in part.

Recently, there have been challenges regarding the protection of access to information in the electoral context. An NGO working with inmates in high-security and maximum-security facilities filed an amparo petition with the TSE, claiming they were unable to stay informed because the prison did not have televisions. This was because the Judge of Guarantees (, or enforcement of the sentence) had so ordered in a resolution. The amparo petition was rejected for lack of standing. Inmates in other types of less restrictive prison regimes do have regulated access to television broadcasts.

Another related case in this area is the one decided by the electoral body in favor of a candidate who, in the middle of the campaign, blocked a user on social media platform X. The complainant argued before the TSE that the block prevented him from accessing campaign information posted by the candidate. In Resolution No. 3252-E1-2018, the body noted that "the information disclosed on these

¹⁹Constitutional Chamber of the Supreme Court of Justice. (2024). *Annual Statistical Compendium*. <https://salaconstitucional.poder-judicial.go.cr/index.php/jurisprudencia/estadistica-por-temas/estadisticas-por-temas-de-asuntos-votados>

platforms, even when related to the group's political agenda, does not render the profile used by the candidate public; that is, its use and management remain private in nature, and therefore the State must refrain from taking any action that limits the autonomy of its owners.”

There are two recent reports on the state of freedom of expression and human rights of this nature in the country. The first was prepared by the UN University for Peace, which is headquartered in Costa Rica. The second was prepared by the University of Costa Rica.

Both agree that recent years have seen a deterioration in the quality of freedom of expression, freedom of the press, and freedom of information, primarily due to practices such as:

- Restrictions or obstacles to access to public information, as public institutions provide data or documents in an illegible or incomplete manner. Additionally, during hearings on key issues—such as disciplinary proceedings for alleged irregular campaign financing—officials invoke their right to remain silent, thereby further reducing the transparency of the information.
- The lack of web accessibility on public institutions' websites constitutes an obstacle to citizens' right to information, affecting people with disabilities, which undermines the guarantee of freedom of expression by limiting their ability to receive quality information.
- Both reports discuss the emergence of fake profiles and anonymous accounts that incite attacks. They document online intimidation against critical journalists by government officials or “trolls.” Another related issue that appears in both reports is the public debate regarding the government's advertising contracts, which benefit certain sectors exclusively, as well as derogatory statements made by official authorities against some media outlets and journalists.

Although some of these situations have been addressed by the constitutional courts, others have gone unprotected or unanswered. The reports suggest that the lack of regulation regarding transparency and content moderation on digital platforms leaves practices such as these unchecked.

3.3 Digital Environment

The most recent report published by the Superintendency of Telecommunications states that, as of 2024, the ratio of mobile phone subscriptions per capita stood at 132%²⁰, corresponding to just over 5 million individual subscriptions to mobile internet services.

An Opensignal report with data from 2024 highlighted the ongoing process regarding the rollout of 5G connectivity in the country²¹, as SUTEL restarted the 5G spectrum auction process, including the 700 MHz, 2.3 GHz, 3.5 GHz, 26 GHz, and 28 GHz bands. In Costa Rica, users of the three main mobile internet providers have 4G coverage at least 73% of the time, and the report indicates that commercial 5G availability is limited, as less than 1% of Liberty Costa Rica users have 5G and are under 5G coverage only 6% of the time at the time of the analysis.²²

Data from DataReportal shows that social media adoption is virtually universal: nearly half of the population aged 18 and older (86.6%) is on at least one social media platform. The average Costa Rican user is ~35 years old and lives primarily in urban areas (approximately 83% of the population

²⁰Telecommunications Superintendency. (2024). *Telecommunications Sector Statistics 2024*. <https://sutel.go.cr/sites/default/files/estadisticas-sector-telecomunicaciones-2024.pdf>

²¹Opensignal. (December 2024). Costa Rica Mobile Network Experience Report – December 2024.

²²WePlan Analytics. (September 2024). *Costa Rica Mobile Quality Report – September 2024*.

is urban). The gender distribution is balanced: women account for ~48–51% of users, and men make up the rest²³.

Geographically, 80% live in cities (primarily in the Greater Metropolitan Area), and the provinces of San José and Alajuela account for the majority of active users. By age, the most active users are teenagers and young adults; for example, studies by Porter Novelli presented in RED 506²⁴ show that the 13–34 age group accounts for nearly 60% of TikTok and social media use in general. On platforms such as TikTok and Instagram, users under 35 predominate, while Facebook is very popular among those over 35. Overall, adoption is growing across all demographic groups, although penetration is higher among younger users for emerging platforms such as TikTok or Snapchat.

As mentioned earlier, a tax reform passed in recent years extended the application of the value-added tax to digital services provided by platforms on a cross-border basis. Although this data could help determine the amounts collected by each platform, consumption per platform, and other relevant details, the information is not broken down. The tax was first collected in October 2020. At that time, the Ministry of Finance reported revenue of \$1.4 million for that month; by August 2025, revenue had reached \$3.2 million²⁵. In other words, in nearly four years, the amount collected by the government from this tax has doubled.

3.4 Digital Platforms Available in the Country

Costa Rica does not have an official registry that legally establishes the platforms' domicile in the country. The only legal obligation applies to services involving a payment that is subject to the tax mentioned in the previous section. According to the Ministry of Finance, as of December 2024, there was a formal list of 161 platforms subject to taxation for the use of their services.

Additionally, starting in 2026, a resolution will take effect requiring platforms to report to the Ministry of Finance the income generated digitally by content creators and similar individuals. The purpose of this is to extend the collection of income tax to these types of individuals. According to Article 1 of the resolution, its purpose is to establish the procedures that Reporting Digital Platform Operators must follow regarding compliance with the registration and reporting obligations related to income earned by sellers in relevant activities that offer lodging, transportation, and personal services through platforms.

The 2022 study published by Porter Novelli identified the distribution of users by platform as follows:

Table 3. Distribution of Users by Digital Platform in Costa Rica

Platform	Number (in millions of users)
WhatsApp	3,524
Instagram	1,934
TikTok	1,777
Facebook	1,754
YouTube	1,734

²³ Kemp, S. (January 2025). *Digital 2025: Costa Rica*. DataReportal. <https://datareportal.com/reports/digital-2025-costa-rica>

²⁴ RED 506. (2022). RED 506 Infographics [Slides]. SlideShare. <https://es.slideshare.net/slideshow/infografasred5062022pdf/253586731>

²⁵ Ministry of Finance. (2025). *VAT Collection on Cross-Border Digital Services*. General Directorate of Taxation.

Platform	Number (in millions of users)
Twitter (X)	0.558

Source: Compiled by the author based on data from Porter Novelli²⁶

Regarding elections, the Supreme Electoral Tribunal has announced the establishment of specific collaboration agreements with digital platforms, primarily Meta. However, signing these agreements does not constitute legal registration or establishment in the country; rather, they serve as communication channels between the electoral body and the platforms for moderating content in response to complaints filed during the campaign.

Although political parties' financial records are public, there is no single list of expenditures made by these groups on digital content and platforms in the electoral context.

3.5 Legislative and Regulatory Context in Costa Rica

3.5.1 Constitutional Framework

The country explicitly guarantees freedom of expression and of the press, the privacy of communications, and access to information in the Constitution. Furthermore, through interpretation, the Constitutional Court has incorporated the Inter-American body of law (*corpus iuris interamericano*) into the legal framework, thereby integrating into the legal system the scope of specific cases, judgments, and advisory opinions of the Inter-American Court related to these fundamental rights. As noted above, constitutional review is centralized.

With regard to the right to rectification and reply, this constitutional protection also applies to private-law entities if it is demonstrated that the violation was to the detriment of private individuals or natural persons; however, recent rulings have denied constitutional protection of this right when the reputation or name of a public institution has been affected.

In electoral matters, the application of this body of constitutional principles has focused on content restrictions and media oversight linked to prohibitions on public officials and other branches of government. This prohibition is set forth in the Electoral Code, which bars government bodies and public institutions in general from promoting their administrative achievements through social media, the media, or any other form of dissemination once elections have been called. A previous interpretation by the TSE had limited this prohibition on digital platform content solely to paid posts. Starting in 2025, the inter-American rulings in *Gadea Mantilla v. Nicaragua* and *Capriles v. Venezuela* were incorporated into electoral case law; consequently, the TSE interpreted that the ban on this type of content should apply regardless of whether or not the institutions paid the platforms.

3.5.2 Telecommunications and Media Legislation

Regulation of the telecommunications sector is governed by the General Telecommunications Law (LGT),²⁷, whose primary objective is to regulate the use and operation of networks and the provision of telecommunications services. This law is based on guiding principles such as universality

²⁶Herrera, K. (2022). *Active Social Media Users in Costa Rica: Overall Geographic, Age, and Gender Distribution* [Infographic]. Profile of the Connected Consumer, RED 506 conference, El Financiero, based on data from Porter Novelli.

²⁷Legislative Assembly of the Republic of Costa Rica. (June 4, 2008). *Law No. 8642. General Telecommunications*. Law. La Gaceta No. 107. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=60840

(guaranteeing a minimum level of services without discrimination) and solidarity (establishing access mechanisms for low-income individuals and special groups).

The LGT defines networks as transmission systems that use various media, including radio waves, cable, and networks used for radio and television broadcasting, as well as cable television networks. It does not refer to digital networks or platforms of this nature. A concession is granted to operate and provide telecommunications networks that require the use of the radio spectrum. For public networks, the concession authorizes the holder to provide all types of telecommunications services available to the public.

With regard to the media and press that use the spectrum (radio and television broadcasting), their use is considered a private activity in the public interest due to its informational, cultural, and recreational aspects. The licensing and provision of these free-to-air services (without a subscription fee) continue to be governed by the Radio Law No. 1758²⁸ and its Regulations.²⁹ However, the networks that support these services are subject to the LGT in areas such as radio spectrum planning and control, access, interconnection, and the sectoral competition regime.

The regulation of digital identity is governed by the Law on Certificates, Digital Signatures, and Electronic Documents (Law No. 8454)³⁰, which applies to all types of transactions and legal acts, both public and private. This law grants functional equivalence to any representative or declaratory statement transmitted by electronic or computer-based means, considering it legally equivalent to physical documents. Electronic documents signed with a digital certificate have the same evidentiary weight as physical documents, although the cost is borne by the user and a device or hardware adapter is required to use them on computers and mobile devices. Specifically, the digital signature—a set of data associated with an electronic document that allows for the verification of its integrity and the identification of the author—has the same value and evidentiary weight as a handwritten signature.

3.5.3 Specific Regulations on Platforms and/or Content Regulation

Until the passage of the Digital Services and E-Commerce Governance Act in April 2026 (see section 3.5.7), the only legal reference to digital platforms was found in the 2018 tax reform, which was limited to the collection of Value-Added Tax.³¹ The new law establishes a comprehensive regulatory framework for the sector, although the other provisions described below remain in effect as components of the broader regulatory framework.

The specific regulations governing legal recognition for tax purposes recognize such transactions under these provisions when they involve the sale of digital or telecommunications services conducted

²⁸Legislative Assembly of the Republic of Costa Rica. (June 19, 1954). *Law No. 1758. Radio Law*. Official Gazette No. 142. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=11646

²⁹Executive Branch of the Republic of Costa Rica. (August 4, 1954). *Executive Decree No. 18. Regulations for the Radio Act*. La Gaceta No. 175. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=11075

³⁰Legislative Assembly of the Republic of Costa Rica. (August 30, 2005). *Law No. 8454. Law on Certificates, Digital Signatures, and Electronic Documents*. La Gaceta No. 197. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=55648

³¹Legislative Assembly of the Republic of Costa Rica. (June 19, 1954). *Law No. 1758. Radio Law*. Official Gazette No. 142. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=11646

via the internet or any other digital platform and processed through an international debit or credit card issuer, or through a provider or intermediary domiciled abroad. This also applies to the sale of intangible services or goods conducted via the internet or any other digital platform and processed through a public or private entity, using a bank account that facilitates payment to the account of a seller or supplier not domiciled in the country.

Another regulatory reference to platforms relates to the regulatory framework for personal data protection. Regulation³² of the Personal Data Protection Act³³ uses the term “Technology Intermediary” or “Service Provider” to refer to any natural or legal person, whether public or private, that provides infrastructure, platform, software, or other services. In this context, responsibility for the processing of personal data rests with the database controller who contracts or subcontracts such services, and the controller must verify that the intermediary complies with the minimum security measures.

3.5.4 Data Protection and Privacy Legislation

Costa Rica does have a specific law on data protection and privacy. This is Law No. 8968, “³⁴” (Law on the Protection of Personal Data and Privacy), whose purpose is to guarantee every person the fundamental right to informational self-determination regarding their private life or activities. The law regulates matters related to the flow of information concerning each person, thereby preventing discriminatory actions. The scope of application covers personal data contained in databases (whether automated or manual), including data stored in the cloud.

The law formalizes informed consent, requiring that the collection of personal data be carried out with the data subject’s express consent, which must be freely given, specific, informed, and unambiguous, and must be documented in writing, either in a physical or electronic document. Consent may be revoked in the same manner, though without retroactive effect. Furthermore, the law prohibits the collection of data without consent, or data obtained through fraudulent, unfair, or unlawful means.

Regarding the application to platforms, the Regulation clarifies that the data controller (the owner or administrator who determines the purpose of the processing) who contracts or subcontracts services from a technology intermediary (platforms, software, infrastructure) remains responsible for the processing of that personal data. Data controllers must implement security measures, and PRODHAB may require compliance with minimum security protocols to verify compliance in response to complaints.

The right of access to information is guaranteed, as is the right to request the rectification, updating, or erasure (deletion) of data. With regard to the right to be forgotten, the retention of personal data that may affect the data subject shall not exceed a period of ten years from the date the purpose of processing ceases, except where otherwise provided by law.

³²Executive Branch of the Republic of Costa Rica. (March 5, 2013). *Executive Decree No. 37541-JP. Regulations for the Law on the Protection of Individuals with Regard to the Processing of Their Personal Data*. La Gaceta No. 45. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=74334

³³Legislative Assembly of the Republic of Costa Rica. (July 7, 2011). *Law No. 8968. Protection of Individuals with Respect to the Processing of Their Personal Data*. La Gaceta No. 170. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=70946

³⁴Legislative Assembly of the Republic of Costa Rica. (July 7, 2011). *Law No. 8968. Protection of Individuals with Regard to the Processing of Their Personal Data*. La Gaceta No. 170. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=70946

3.5.5 Specific Regulations on the Protection of Vulnerable Groups

First, Law No. 10267³⁵ prohibits the dissemination of propaganda that degrades the dignity, honor, and image of older adults or that promotes myths and/or stereotypes against old age and the aging process. The scope of application is explicit, as it includes propaganda intended for social media, video games, digital services, or other online platforms, as well as downloadable audiovisual material. The Propaganda Control Office (OCP) may order the immediate removal of such propaganda as a precautionary measure.

The second area of protection concerns acts of gender-based violence in commercial advertising (whether digital or analog). Law No. 5811³⁶ controls and regulates commercial advertising that offends dignity or family modesty, or that uses the image of women in an immodest manner to promote sales. Press, radio, film, and television companies (and, in general, all entities that operate an individual or collective medium of communication) are secondarily liable for violations. Such advertising must have the prior and express approval of the OCP. The law also stipulates that advertising that offends dignity or is indecent is absolutely prohibited in programs or activities aimed at minors.

Finally, the General Telecommunications Law prohibits the use of automated voice, fax, or email calling systems for direct sales purposes without the prior consent of users. Furthermore, it is prohibited to send direct sales emails that disguise or conceal the sender's identity.

3.5.6 Digital Election Regulation

Costa Rica does not have a regulatory framework addressing disinformation in election campaigns; rather, the issue has been addressed primarily through the case law of the TSE. There are at least two areas on which this legal interpretation focuses.

The first concerns the prohibition imposed on government institutions regarding the publicization of achievements and the promotion of their actions during the campaign period. In Resolution No. 4190-E8-2025³⁷, the TSE ruled to clarify its interpretation of the scope of Article 142 of the Electoral Code³⁸, stipulating that institutions must comply with the restriction in both traditional media and institutional digital media and platforms, regardless of whether payment is involved.

Furthermore, the agency recognizes the purchase of services and advertising on digital platforms as a campaign expense; to this end, it requires each political party to provide the links or accounts they will use during the election campaign and through which such advertising will be purchased.

³⁵Legislative Assembly of the Republic of Costa Rica. (July 11, 2022). *Law No. 10267. Law Prohibiting the Dissemination of Propaganda That Degrades Older Adults*. The Official Gazette No. 172. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=97727

³⁶Legislative Assembly of the Republic of Costa Rica. (October 10, 1975). *Law No. 5811. Law on the Office of Propaganda Control*. La Gaceta No. 202. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=11077

³⁷Supreme Electoral Tribunal of the Republic of Costa Rica. (June 20, 2025). *Resolution No. 4190-E8-2025. Adjustment of criteria regarding the use of digital platforms by public institutions to disseminate information on government administration during the campaign period*. <https://tse.go.cr/imgs/info/4190-E8-2025.pdf>

³⁸Legislative Assembly of the Republic of Costa Rica. (September 2, 2009). *Law No. 8765. Electoral Code*. La Gaceta No. 171, Supplement No. 37. <https://www.tse.go.cr/normativa/codigoelectoral>

3.5.7 The Digital Services and E-Commerce Governance Act (2026): A Regulatory Milestone

On April 16, 2026, the Legislative Assembly of Costa Rica approved the Law on the Governance of Digital Services and E-Commerce (Bill No. 23,184) in its second reading, making the country the first in Central America to have a comprehensive legal framework designed to regulate digital platforms and services. The law will take effect twelve months after its publication in the Official Gazette, **La Gaceta**, during which time market participants must adapt their operations to the new regulatory framework.

The bill, originally introduced in 2022 by Representative Kattia Cambronero Aguiluz and other legislators, was inspired by two leading international models: the UNCITRAL Model Law on Electronic Commerce and the European Union's E-Commerce Directive, as well as the European Union's proposed Digital Services Act (DSA). Following a process that included the issuance of a technical-legal opinion in 2023, a unanimous affirmative opinion from the Special Standing Committee on Science, Technology, and Education in April 2024, and the incorporation of twenty-four approved motions out of a total of forty-six submitted, the final text was adopted in 2026.

The law is structured around four substantive pillars. The first regulates e-commerce and imposes transparency obligations on online merchants: full identification of the seller, a detailed description of the product or service, a complete breakdown of the price, and confirmation prior to the transaction; furthermore, it expressly prohibits so-called “dark patterns”—interface designs that induce consumers to make unwanted decisions. The second pillar establishes a liability regime for digital intermediaries—hosting platforms, search engines, and others—inspired by the “safe harbor” model: liability is limited provided specific requirements are met, including the implementation of mechanisms for reporting illegal content and internal complaint systems. The third pillar strengthens the protection of personal data, with mandatory security measures, restrictions on the use of data from children under thirteen for advertising purposes, and explicit protection of end-to-end encryption. Finally, the fourth pillar regulates digital advertising: mandatory identification of ads, disclosure of funding sources, transparency regarding targeting criteria, and a ban on unsolicited commercial communications.

The law also includes specific provisions for the fintech sector: companies must implement secure electronic payment systems, report on applicable security levels and certifications, and ensure immediate notification of each transaction. In terms of penalties, serious violations can result in fines of approximately 42,500 U.S. dollars.

From the perspective of alignment with the UNESCO Guidelines on the Governance of Digital Platforms, the passage of this law represents the most significant regulatory advance in Costa Rica in the area of digital governance. The UNESCO Guidelines articulate their requirements around pillars such as platform transparency and accountability, the protection of user rights, mechanisms for effective redress, and independent oversight. On several of these fronts, the new law constitutes concrete progress: for the first time, Costa Rica has a regime of limited liability for digital intermediaries—aligned with the principle that platforms should not be immune from all liability, nor should they bear absolute responsibility for third-party content—as well as explicit transparency standards for consumers and mandatory complaint mechanisms. The ban on “dark patterns” is particularly relevant from the perspective of user rights, as it directly addresses the manipulative design practices that the Guidelines identify as a threat to autonomy and informed decision-making. Equally noteworthy is the explicit protection of end-to-end encryption, which strengthens guarantees of privacy and freedom of communication against potential state interference.

However, a rigorous comparison with the UNESCO Guidelines reveals areas of requirement that the law does not address. First, the Guidelines require States to promote algorithmic transparency: platforms must be able to explain how their recommendation, ranking, and automated moderation systems affect users and the public sphere. The approved law is silent on this issue: it does not

establish obligations for algorithm audits, does not require explainability of recommendation systems, and does not provide for mechanisms for independent oversight of the platforms' internal operations.

Second, the Guidelines promote the management of systemic risks—periodic assessments of the impact of platforms on human rights, public health, or electoral integrity—an aspect absent from the Costa Rican law.

Third, while the law requires intermediaries to implement mechanisms for reporting illegal content, it does not define a content moderation regime that guarantees due process for affected users: prior notification, the possibility of appeal, and transparency regarding the criteria applied, as required by the Guidelines in their provision safeguarding freedom of expression.

Finally, fourth, the law also fails to establish an independent regulatory body with specific jurisdiction over digital platforms, leaving enforcement of the law in the hands of general-purpose institutions whose specialized technical capacity is not guaranteed.

Overall, the Digital Services and E-Commerce Governance Act positions Costa Rica as a regional leader: it is the first Central American country with a comprehensive framework of this nature and goes significantly further than what any other country in the region—except for Panama in the electoral sphere and Mexico with its own regulations—has achieved to date. The twelve-month *vacatio legis* period represents a strategic opportunity for civil society, academia, and the country's institutions to promote the development of complementary regulations that address the remaining gaps: in particular, the regulation of algorithmic systems, content moderation with due process safeguards, and the creation of a supervisory authority with sufficient independence and technical capacity to engage with major platforms on an equal footing. Without these complementary elements, the regulatory framework will remain incomplete in light of the most demanding standards of international digital governance.

3.6 Alignment with UNESCO Guidelines: Costa Rica

An analysis of Costa Rica's alignment with UNESCO's guidelines reveals that the country has a robust constitutional framework—both substantive and procedural—that guarantees access to information, freedom of expression and of the press, privacy of communications, and the right to telecommunications.

Through constitutional interpretation, it has been established that international treaties and conventions that expand fundamental rights, together with Inter-American case law, take precedence over the Constitution itself and are immediately applicable. This ensures a solid legal foundation for protecting individual and collective freedoms.

However, the effective protection of these rights faces significant operational challenges, as claims are concentrated exclusively in the Constitutional Chamber—a system that, while free of charge and free of formalities, suffers from marked territorial centralization. Added to this is a significant regulatory gap, as the country lacks specific regulations on content moderation on digital platforms and on consumer protection in the context of cross-border digital services.

In the absence of a comprehensive sector-specific law defining clear criteria for content restrictions, the application of the principles of legality, necessity, and proportionality falls to the Constitutional Chamber's case-by-case analysis. Case law requires that any restriction on freedoms be grounded in a public, clear, and accessible law, and that the measure adopted be appropriate, foreseeable, and as least harmful as possible.

In practice, current restrictions stem from scattered regulations in areas such as criminal law, electoral law, and data protection. This lack of a single statutory definition creates a fragmented regulatory

landscape, where different authorities apply varying criteria depending on whether the focus is on taxation, telecommunications, or elections.

With the passage of the Digital Services and E-Commerce Governance Act (2026), Costa Rica has, for the first time, incorporated a regime of limited liability for digital platforms inspired by the “safe harbor” model: intermediaries’ exemption from liability is subject to compliance with specific legal requirements, including the implementation of mechanisms for reporting illegal content and internal complaint systems. This represents a substantial improvement over the previous situation. However, in the electoral sphere, the problem persists: the Supreme Electoral Tribunal (TSE) continues to rely on voluntary cooperation agreements with platforms and lacks its own enforcement tools to address potential violations related to digital campaigns.

The new Digital Services Act of 2026 makes progress on some of these fronts: it imposes transparency obligations regarding terms and conditions and establishes complaint systems for users. However, significant gaps remain: the law does not include algorithmic audit requirements, does not provide for systemic risk management obligations, and does not regulate transparency regarding the operation of recommendation systems. In this regard, the resulting framework is more comprehensive than the previous one, but it remains less stringent than the standards set by other laws—such as the European Digital Services Act—with respect to obligations regarding the internal operations of platforms.

Furthermore, although there are constitutional principles against arbitrary suspensions, there is no specific regime that expressly prohibits government-imposed platform blocks without an enforceable judicial procedure, nor is there a general provision regulating these companies’ monitoring obligations.

Regarding the protection of vulnerable groups, while there are specific criminal laws and regulations that protect minors, women, and older adults from offensive propaganda or exploitation, there are no direct sector-specific obligations requiring platforms to implement preventive mechanisms such as filters or age verification.

A similar situation exists in the fight against disinformation, which is managed primarily by the TSE on a temporary basis during electoral processes through voluntary agreements, without constituting permanent regulations.

Finally, the legal framework does not require platforms to provide empowerment tools to users, leaving digital literacy to national strategies and public policies that operate as isolated initiatives and have not yet achieved widespread coverage.

4. Country Analysis: El Salvador

4.1 Political and Legal System

El Salvador's regulatory and political framework is based on its 1983 Constitution of the Republic³⁹, which, in Article 1, expressly recognizes the human person as the origin and supreme purpose of all State activity, and states that the State is organized to achieve justice, legal certainty, and the common good. Article 85 of the Constitution defines the country as a sovereign state and explicitly establishes its form of government as republican, democratic, and representative.

The Salvadoran political system is pluralistic and has evolved legally toward greater democratic openness; through regulations such as the Provisions for the Nomination of Non-Partisan Candidates (Decree 555)⁴⁰, which recognized the right of citizens to run for legislative office as independents, thereby strengthening the freedom to exercise the right to free, direct, equal, and secret suffrage enshrined in Article 78 of the Constitution.

At the constitutional level, the exercise of public power is delegated to three fundamental branches that operate under a strict principle of non-delegability and mutual collaboration: the Legislative Branch, exercised by a unicameral Legislative Assembly with the authority to enact laws and elect second-tier officials; the Executive Branch, headed by the Presidency of the Republic; and the Judicial Branch, whose highest authority is the Supreme Court of Justice. Within the latter, the Constitutional Chamber plays a central role as the highest and final interpreter of the Constitution, resolving disputes and safeguarding fundamental rights through proceedings for unconstitutionality, amparo, and habeas corpus (including *habeas data* for the protection of personal information).

In the political-electoral sphere, the highest administrative and judicial authority is the Supreme Electoral Tribunal (TSE), which is responsible for convening, organizing, conducting, and supervising all elections, acting as the final arbiter in disputes of this nature and in the oversight of political parties. Currently, the Salvadoran electoral system is undergoing a phase of profound technological and demographic transformation driven by the recent Special Law on the Exercise of the Right to Vote Abroad (Decree 541 of 2022)⁴¹, which integrated the vast Salvadoran diaspora into the democratic process through the pioneering implementation of remote electronic voting via the internet and in-person electronic voting.

Beyond the three traditional branches of government, the institutional design of the Salvadoran state includes a Public Ministry comprising the Attorney General's Office, the Office of the General Prosecutor, and the Office of the Human Rights Ombudsman (PDDH). This latter entity holds the constitutional mandate to ensure unrestricted respect for citizens' fundamental rights in the face of possible abuses or omissions by public authorities, functioning as a moral and institutional watchdog.

³⁹El Salvador. (December 15, 1983). *Constitution of the Republic of El Salvador*. Official Gazette No. 234. <https://www.asamblea.gob.sv/node/8291>

⁴⁰Legislative Assembly of the Republic of El Salvador. (November 4, 2010). *Decree No. 555. Provisions for the Nomination of Non-Partisan Candidates in Legislative Elections*. Official Gazette No. 222, Volume No. 389. <https://www.asamblea.gob.sv/node/628>

⁴¹Legislative Assembly of the Republic of El Salvador. (October 18, 2022). *Special Law on Voting Abroad*. Official Gazette No. 197, Volume No. 437. <https://www.asamblea.gob.sv/node/12437>

4.2 Freedom of Expression and Human Rights

Civil and political rights are primarily grounded in Article 6 of the Constitution, which categorically guarantees that every person may freely express and disseminate their thoughts by any means, without being subject to prior censorship. This freedom, however, is subject to legitimate constitutional limits when its exercise subverts public order or infringes upon the morals, honor, or private life of third parties—legal rights that are expressly protected under Article 2.

For its part, Article 24 enshrines the inviolability of postal correspondence and the unbreakable secrecy of telecommunications, establishing that their interception may only be carried out in exceptional cases and strictly pursuant to a reasoned judicial order. Furthermore, Article 18 recognizes the right of citizens to petition any constituted authority.

Despite the strength of these formal guarantees, the full and secure exercise of freedom of expression faces its most serious and systematic challenges since the signing of the Peace Accords. In 2024, Reporters Without Borders ranked El Salvador at an alarming 133rd out of a total of 180 countries.⁴² This profound deterioration has been exacerbated by the uninterrupted enforcement of a State of Emergency, in effect since March 2022, which de facto suspends vital constitutional guarantees (including the inviolability of telecommunications and the right to a defense), creating an environment of high vulnerability for citizens.

In this climate of exceptional circumstances, criminal reforms—dubbed a “Gag Law” by the journalism community—were passed, imposing severe prison sentences of up to fifteen years on anyone who reproduces or transmits messages originating from gang groups through the media or digital platforms.⁴³ This had an immediate chilling effect, forcing the media into self-censorship, although this practice was decriminalized in 2023.⁴⁴

Digital security and privacy have become matters of grave concern. Numerous international investigations have documented the covert use of military spyware (such as Pegasus) to hack into the devices of investigative journalists, activists, and opposition figures.⁴⁵ Added to this technical surveillance is the proliferation of online disinformation campaigns, revealing the systematic operation of armies of fake accounts and *troll* farms in the country.⁴⁶

4.3 Digital Environment

El Salvador shows continuous growth in its connectivity indicators at the macroeconomic level. However, there is an underlying structural digital divide that chronically marginalizes rural areas and lower-income groups. Mobile connectivity via cell phones has become the primary means of internet access for the majority of the population, in a context where fixed-line access remains limited.

⁴²Reporters Without Borders. (n.d.). *El Salvador*. Retrieved February 25, 2026, from <https://rsf.org/es/pais/el-salvador>

⁴³Committee to Protect Journalists. (April 8, 2022). *New law adopted in El Salvador imposes prison sentences of up to 15 years on journalists who report on gangs*. <https://cpj.org/es/2022/04/nueva-ley-adoptada-en-el-salvador-sanciona-con-penas-de-hasta-15-anos-de-prision-a-los-periodistas-que-den-cobertura-informativa-a-las-pandillas/>

⁴⁴Legislative Assembly of El Salvador. (November 2, 2023). *Lawmakers decriminalize the dissemination of messages generated by gangs*. <https://www.asamblea.gob.sv/node/12992>

⁴⁵Amnesty International. (January 13, 2022). *El Salvador: Amnesty International verifies the use of the Pegasus spyware program to surveil journalists*. <https://www.amnesty.org/es/latest/news/2022/01/el-salvador-pegasus-spyware-surveillance-journalists/>

⁴⁶Human Rights Watch. (2024). *El Salvador*. In *World Report 2024*. Retrieved February 25, 2026, from <https://www.hrw.org/es/world-report/2024/country-chapters/el-salvador>

According to recent reports on the country's digital ecosystem, there are approximately 11 million mobile connections in a country with a population of just over 6 million,⁴⁷ which translates to penetration levels of around 170% due to the widespread use of multiple SIM cards per person.⁴⁸ At the same time, fixed-line broadband internet subscriptions barely exceed a few hundred thousand, confirming that the mobile phone is the sole channel for internet access for large segments of the population.⁴⁹

El Salvador has built a narrative of financial and technological innovation based on the adoption of Bitcoin⁵⁰ as legal tender and the launch of a state-run digital wallet called ChivoWallet.⁵¹ However, the reality is more nuanced: although mobile and fixed-line download speeds have improved in recent years, El Salvador continues to lag behind other countries in the region, with a persistent gap between broadband penetration and mobile line penetration,⁵² suggesting that the push for cryptocurrencies has not been accompanied by investments in network infrastructure.

The Salvadoran telecommunications market is highly concentrated, with two major transnational operators, Tigo and Claro, holding dominant positions in mobile telephony and consumer internet access.⁵³ Sector statistics show that these two providers account for the majority of mobile lines and broadband subscriptions, while the rest of the market is divided among other smaller players⁵⁴. The business model is primarily based on prepaid service, with approximately 90% of mobile lines offered under this model, and top-ups being the predominant mechanism for data access and consumption. In February 2024, the Salvadoran government granted the satellite internet company Starlink a 10-year concession for satellite internet frequencies, allowing the company to offer this service commercially.⁵⁵

In this context, operators have repeatedly rolled out mobile data offers under a *zero-rating* or tiered pricing scheme that includes access to applications—particularly Meta's (Facebook or WhatsApp) and⁵⁶—targeted primarily at prepaid users. This allows users to access these platforms without the traffic counting toward their general data allowance, making accessible internet more expensive. These practices have been identified as de facto violations of the principles of net neutrality, limiting people's ability to access the open internet and to verify information through diverse sources.⁵⁷

⁴⁷International Trade Administration. (2024). *El Salvador - Information and Communications Technology*. U.S. Department of Commerce. <https://www.trade.gov/country-commercial-guides/el-salvador-information-and-communications-technology>

⁴⁸Kemp, S. (November 8, 2025). *Digital 2026: El Salvador*. DataReportal – Global Digital Insights. <https://datareportal.com/reports/digital-2026-el-salvador>

⁴⁹International Telecommunication Union. (August 2023). Digital Development Dashboard BETA: El Salvador. https://www.digitaldevelopment.org/wp-content/uploads/2023/08/ddd_SLV-1.pdf

⁵⁰National Council for Financial Inclusion and Education. (n.d.). *Bitcoin in El Salvador*. Retrieved February 25, 2026, from <https://inclusionfinanciera.gob.sv/bitcoin-en-el-salvador/>

⁵¹Chivo Wallet. (n.d.). *Home*. Retrieved February 25, 2026, from <https://www.chivowallet.com/>

⁵²International Telecommunication Union. (August 2023). Digital Development Dashboard BETA: El Salvador. https://www.digitaldevelopment.org/wp-content/uploads/2023/08/ddd_SLV-1.pdf

⁵³International Trade Administration. (2024). *El Salvador - Information and Communications Technology*. U.S. Department of Commerce. <https://www.trade.gov/country-commercial-guides/el-salvador-information-and-communications-technology>

⁵⁴Internet Society. (2026). *Country report for El Salvador*. Internet Society Pulse. Retrieved February 25, 2026, from <https://pulse.internetsociety.org/en/reports/SV/>

⁵⁵Thomson Reuters. (February 28, 2024). *El Salvador grants Musk's Starlink unit a concession for satellite internet*. COOL FM. <https://wqxc.com/2024/02/28/el-salvador-grants-musks-starlink-unit-concession-for-satellite-internet/>

⁵⁶Galpaya, H. (February 23, 2017). *Zero-rating in emerging economies* (Global Commission on Internet Governance Paper Series No. 47). Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/GCIG%20no.47_2.pdf

⁵⁷Massé, E., Björkstén, & Chima, R. J. S. (June 4, 2016). *Zero rating: A global threat to the open internet*. Access Now. <https://www.accessnow.org/zero-rating-global-threat-open-internet/>

4.4 Digital Platforms Available in the Country

In 2025, El Salvador had approximately 3.90 million active social media users, equivalent to more than 61% of the total population and more than 87% of the population over the age of 18. These figures show a consolidation of the digital landscape compared to 2023 data, when 4 million active users were reported, comprising 51.9% women and 48.1% men.⁵⁸

In terms of platform reach, the Meta ecosystem and video platforms account for the majority of the audience. By 2025, Facebook reports approximately 4.05 million potential users for advertising campaigns, representing an increase from the 3.6 million reach reported in 2023. For its part, Instagram has nearly 1.8 million users, and Messenger maintains a significant presence in daily communication. In the audiovisual format, YouTube reaches 3.58 million Salvadorans, maintaining stable figures compared to previous years, while TikTok is experiencing exponential growth and high penetration, especially among younger demographic segments.⁵⁹

The concentration of news consumption on a few platforms shapes the population's digital habits in a context where internet access is primarily via mobile devices. Social media platforms operate not only as spaces for entertainment or personal interaction but also shape the way Salvadorans access news and engage in political debate. Additionally, these applications are fundamental to the country's economic activity, serving as primary channels for advertising campaigns, informal commerce, and online transactions.⁶⁰

4.5 Legislative and Regulatory Context in El Salvador

4.5.1 Constitutional Framework

Article 6 of the Constitution of El Salvador enshrines the inalienable right of every person to freely express and disseminate their thoughts. By protecting the expression of thought “by any means” and expressly prohibiting prior censorship, this provision applies the principle of “technological neutrality,” which automatically protects expressions posted on the internet, digital platforms, and social media.

However, the Constitution itself acknowledges that this right is not absolute. Articles 2 and 24 serve as necessary constitutional safeguards against potential abuses or disproportionate interventions. Article 2 protects the right to honor, personal and family privacy, and one's own image, serving as a safeguard against harmful conduct such as defamation or cyberbullying. For its part, Article 24 safeguards citizens' privacy by guaranteeing the strict inviolability of correspondence and prohibiting interference with telecommunications. This provision establishes a framework of safeguards, stipulating that any interception of electronic or telematic communications may only be carried out on an exceptional and temporary basis, pursuant to a duly reasoned judicial order, and exclusively for the purpose of investigating serious crimes.

In the absence of a general data protection law in the country, the established case law of the Constitutional Chamber of the Supreme Court of Justice has assumed a leading protective role. This highest court has interpreted the protective provisions of Article 2 broadly and in a manner that safeguards rights to recognize and operationalize the right to informational self-determination through

⁵⁸Márquez, D. (June 10, 2025). DataReportal and Internet and Social Media Use in El Salvador 2025. iLifebelt. <https://ilifebelt.com/datareportal-y-el-uso-de-internet-y-redes-sociales-en-el-salvador-2025/2025/06/>

⁵⁹Pulso. (2025, June 16). *Internet and Social Media Use in El Salvador 2025*. Pulso Capital. <https://pulsocapital.com/uso-de-internet-redes-sociales-el-salvador-2025/>

⁶⁰Calderón, S. (October 15, 2024). *More than 50% of Salvadorans spend more than three hours a day on social media*. Diario El Mundo. <https://diario.elmundo.sv/economia/mas-50-de-los-salvadorenos-pasa-mas-de-tres-horas-diarias-en-redes-sociales>

the legal remedy of *Habeas Data*. Through this mechanism of judicial protection, Salvadoran citizens have been granted the constitutional authority to control their personal and sensitive information when it is stored, profiled, or processed in databases, regardless of whether these are managed by public institutions, private corporations, or large technology platforms.

Finally, this set of civil and privacy rights is complemented by constitutional mandates regarding the economic order and social welfare (Articles 101 and 102). These provisions oblige the State to promote economic and technological development, as well as to actively defend the interests of consumers.

It is this constitutional foundation that has legitimized the creation of secondary regulations applicable to the online environment—such as laws on e-commerce and consumer protection—to combat misleading advertising and regulate unfair terms in the platforms’ “Terms and Conditions.” Thus, the Salvadoran constitutional framework not only protects users in the realm of communication but also imposes on the State the duty to create the legal certainty necessary for equitable digital coexistence.

That said, there are concerns that a restrictive digital environment has taken shape in El Salvador. As mentioned earlier, stigmatization campaigns driven by *troll* farms can discredit the work of the independent press and civil society organizations, but they can also have a paralyzing effect on citizens, who are increasingly opting for self-censorship on platforms out of fear of legal reprisals, arrests under a state of emergency, or virtual lynchings. The very nature of the digital infrastructure—based primarily on prepaid mobile access and *zero-rating* schemes—does not help the situation either, as it raises doubts about the effective guarantee of the right to information. Thus, the Salvadoran internet ecosystem, which constitutionally should function as a pluralistic and secure extension of the public sphere, suffers from a power imbalance that makes it particularly vulnerable to digital intimidation, to the detriment of freedom of expression.

4.5.2 Telecommunications and Media Legislation

The regulatory framework governing connectivity infrastructure and communications in El Salvador is anchored in the Telecommunications Law (Legislative Decree 142 of 1997).⁶¹ This legislation delegates to the General Superintendency of Electricity and Telecommunications (SIGET) the technical and institutional authority for the administration, regulation, and granting of concessions for the radio spectrum, which is considered a state resource. This law, dating from the end of the last century, prioritizes technical regulation, frequency management, and the promotion of market competition under SIGET’s administrative supervision. It lacks provisions to regulate and guarantee net neutrality, transparent data traffic management, or the liability regime for intermediaries and digital platforms. One historical control mechanism that stands out for its political impact is Article 127 of this law, which unequivocally requires all radio frequency concessionaires to broadcast simultaneous “national broadcasts” when called upon by the Office of the President, under penalty of severe fines for noncompliance, thereby perpetuating and legalizing the Executive Branch’s monopolistic control over the mass media spectrum in specific situations.

Beyond the management of frequencies for traditional radio and television, this law laid the groundwork for opening up data transmission services to free competition, regulating network interconnection and access to essential resources. In the digital age, SIGET’s regulatory role is significant, as its operational and technical regulations regarding telecommunications infrastructure directly impact the quality, coverage, and accessibility of internet services for the Salvadoran population. In terms of legislation on telecommunications, media, and the press, the country is primarily governed by the Telecommunications Law, enacted by Legislative Decree 142 of 1997.

⁶¹Legislative Assembly of the Republic of El Salvador. (May 22, 1997). *Decree No. 142. Telecommunications Law*. Official Gazette No. 108, Volume No. 335. <https://www.asamblea.gob.sv/node/634>

In the realm of public oversight and the relationship between the State and society, the Law on Access to Public Information (Legislative Decree 534 of 2011)⁶² formally recognizes that the right to freedom of expression includes the inalienable right to seek, receive, and disseminate information regardless of borders and by any means, expressly including electronic means. To implement this mandate, the legislation establishes the principle of “maximum disclosure,” requiring all state institutions and municipalities to proactively publish information *ex officio* through websites and transparency portals. The Institute for Access to Public Information (IAIP) is the body responsible for safeguarding citizens’ right to know. This institute implements these mandates through the aforementioned Decree 534 of 2011, based on the premise that transparency is a fundamental condition for citizen participation. The IAIP is responsible for ensuring that every person can seek, receive, and disseminate information derived from government operations, while safeguarding accountability and protecting confidential personal data held by the public administration.

However, as noted, despite the doctrinal robustness of these guarantees, Legislative Decree No. 333 (which declares a state of emergency in El Salvador)⁶³ suspends Articles 7 and 24 of the Salvadoran Constitution. This seriously undermines journalistic practice and freedom of expression by suspending the inviolability of correspondence and telecommunications (Art. 24), as well as freedom of association (Art. 7). By allowing the State to intercept and examine private communications without the need for a prior, reasoned court order, the confidentiality of communications is destroyed and professional secrecy is violated, preventing journalists from protecting the identity of their sources. This unrestricted surveillance, combined with the suspension of the right to legal defense and the extension of administrative detention to 15 days (Arts. 12 and 13), leaves journalists and critical voices defenseless, which also creates a climate of vulnerability for citizens in both the physical and digital civic spheres. In this context of exceptional circumstances, the imposition of criminal reforms such as the “Muzzle Law”—which threatened up to fifteen years in prison for anyone who reproduced gang messages on digital platforms or in traditional media—triggered a profound chilling effect and forced widespread self-censorship within the news ecosystem; a structural coercion whose paralyzing effects persist even though the dissemination of such messages was decriminalized in 2023.

In the digital realm, the suspension of Article 24 *de facto* legitimizes massive and arbitrary state surveillance of cyberspace. By removing the constitutional protections for telecommunications, the government is empowered to intercept emails, instant messaging apps, data traffic, and social media profiles without judicial oversight. This has a severely negative impact on *online* freedom of expression, as it creates an environment of hyper-surveillance where citizens assume that their digital footprint and political opinions on the internet are being constantly monitored.

4.5.3 Specific Regulation of Platforms and/or Content Regulation

El Salvador does not have a single, comprehensive digital code or a modern law that classifies and regulates social media platforms as information intermediaries. In the absence of such legislation, the current and applicable regulatory framework operates through various legal instruments.

In the realm of civil and commercial law, regulation is addressed tangentially through legislation such as the Electronic Signature Act (Legislative Decree 133)⁶⁴ and the Electronic Commerce Act

⁶²Legislative Assembly of the Republic of El Salvador. (April 8, 2011). *Decree No. 534. Law on Access to Public Information*. Official Gazette No. 70, Volume No. 391. <https://www.asamblea.gob.sv/node/624>

⁶³Legislative Assembly of the Republic of El Salvador. (March 27, 2022). *Decree No. 333. State of Emergency*. Official Gazette No. 59, Volume No. 434. <https://www.asamblea.gob.sv/node/12105>

⁶⁴Legislative Assembly of the Republic of El Salvador. (October 22, 2015). *Decree No. 133. Electronic Signature Act*. Official Gazette No. 201, Volume No. 409. <https://www.asamblea.gob.sv/node/623>

(Legislative Decree 463).⁶⁵ These tools provide the necessary framework to legally validate transactions, online contracts, and data messages, enabling commercial development and secure interactions in the digital environment.

In the area of criminal law, the regulation of online threats falls under the Special Law Against Computer Crimes and Related Offenses, enacted by Legislative Decree 260 in 2016.⁶⁶ This legislation serves as the government's primary tool for criminalizing and punishing unlawful conduct such as computer fraud, unauthorized access to systems, sabotage, and the acquisition or transfer of confidential information.

To address the imbalance between technology companies and citizens, the government also relies on the Consumer Protection Law as a supplementary measure.⁶⁷ This law applies to virtual environments, as it prohibits misleading advertising and strictly regulates “adhesion contracts”—the legal framework under which the “Terms and Conditions” of digital platforms operate. Under this law, any abusive clauses that seek to exempt service providers from liability or that impose arbitrary waivers of rights on users are declared null and void, providing a basic layer of legal protection against corporate abuses.

The Salvadoran legal system does not provide for a liability exemption scheme for platforms regarding content uploaded or shared by their users. Since there is no precise definition of the civil or criminal liability of internet service providers for illegal or harmful posts by third parties, content moderation operates in a legal vacuum. Nor do technology platforms have transparency policies or mechanisms for appeals and due process.

However, any analysis of platform governance and digital content creation in El Salvador must be situated within the context of the current, aforementioned State of Emergency, which has drastically altered the rules of the digital ecosystem by suspending constitutional guarantees—in particular, the secrecy of telecommunications (Art. 24 of the Constitution)—and which continues to be extended⁶⁸. The State of Emergency, as it has now persisted over time, *de facto* legalizes unrestricted state surveillance, allowing authorities to intercept electronic communications, monitor private messaging, and track data traffic on social media without the need for a prior court order or judicial oversight.

This erosion of digital privacy, combined with the absence of a General Law on the Protection of Personal Data, leaves platform users completely defenseless against the state apparatus.

The direct result of this state of emergency is self-censorship driven by a well-founded fear that political opinions, social media interactions, or shared content could be used to justify arbitrary administrative detentions (under the very suspension of rights). This situation imposes serious governmental barriers to the internet serving as a free space for democratic debate in the country.

4.5.4 Data Protection and Privacy Legislation

Salvadoran legislation on data protection and citizen privacy faces a structural gap in El Salvador. To date, the country lacks a personal data protection law that is binding on the private sector, as well as

⁶⁵Legislative Assembly of the Republic of El Salvador. (October 22, 2020). *Decree No. 463. Electronic Commerce Act*. Official Gazette No. 215, Volume No. 429. <https://www.asamblea.gob.sv/node/10852>

⁶⁶Legislative Assembly of the Republic of El Salvador. (February 4, 2016). *Decree No. 260. Special Law Against Cybercrimes and Related Offenses*. Official Gazette No. 29, Volume No. 410. <https://www.asamblea.gob.sv/node/621>

⁶⁷Legislative Assembly of the Republic of El Salvador. (August 31, 2005). *Decree No. 772. Consumer Protection Law*. Official Gazette No. 166, Volume No. 368. <https://www.asamblea.gob.sv/node/630>

⁶⁸Inter-American Commission on Human Rights. (August 14, 2025). *El Salvador: IACHR reiterates concern over the excessive prolongation and improper application of the state of emergency*. Organization of American States. <https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2025/162.asp>

a specialized national authority dedicated exclusively to this matter. Given this legal void, the control and safeguarding of citizen information operate in a highly fragmented manner.

Protection, as in other countries without specific legislation, is based primarily on the constitutional jurisprudence of *Habeas Data*. Meanwhile, in the sphere of government administration, the aforementioned Law on Access to Public Information (Legislative Decree 534) provides protection for “confidential personal data,” but its scope is strictly limited, since the Institute for Access to Public Information (IAIP) has jurisdiction and the authority to impose sanctions only over information held by government agencies and institutions.

To address the lack of regulation regarding the mass processing of data by corporate entities and technology platforms, the State must rely on sector-specific tools. In this regard, the aforementioned Consumer Protection Law serves as a legal check against the commodification of privacy. This legislation seeks to penalize the abusive transfer and unauthorized commercialization of commercial, credit, or consumer personal data by companies. Although it provides users with a basic defense against the exploitation of their information in the market for goods and services, it is an insufficient measure to address the complexity of algorithmic profiling and the mass collection of metadata characteristic of the modern digital ecosystem.

Finally, in the sensitive area of investigative privacy and surveillance, the country is governed by the Special Law on Telecommunications Interception (Legislative Decree 285).⁶⁹ This law implements the constitutional exception by permitting the interception of electronic and telematic communications for the prosecution of serious crimes, centralizing the technical protocols for wiretapping under strict adherence to a warrant issued by a specialized judge.

However, despite a legal framework that, *on the face of it*, appears to protect civil liberties, operational practice reveals a diametrically opposed reality. International organizations have repeatedly warned about the lack of sufficient independent technical controls to audit the use of communications interception systems⁷⁰, which has led to serious and repeated violations of privacy. Internationally documented reports on the use of technological spyware against political figures, human rights defenders, and journalists highlight the alarming fragility of state safeguards and the imminent risk that these tools will be used for political persecution.⁷¹

4.5.5 Specific Regulations for the Protection of Vulnerable Groups

The protection of vulnerable populations in El Salvador’s digital ecosystem is structured through an approach that combines preventive measures and criminal prosecution. In the area of prevention, the “Growing Together” Law for the Comprehensive Protection of Infants, Children, and Adolescents⁷² incorporates modern guidelines aimed at safeguarding minors from access to and exposure to online content of a violent, sexual, or harmful nature that could impede their development.

⁶⁹Legislative Assembly of the Republic of El Salvador. (March 4, 2010). *Decree No. 285. Special Law on Telecommunications Interception*. Official Gazette No. 45, Volume No. 386. <https://www.asamblea.gob.sv/node/633>

⁷⁰UN. (July 19, 2021). *Governments cannot use technologies to spy on citizens that violate human rights*. United Nations. <https://news.un.org/es/story/2021/07/1494542>

⁷¹Amnesty International. (January 13, 2022). El Salvador: Amnesty International verifies the use of the Pegasus spyware program to monitor journalists. <https://www.amnesty.org/es/latest/news/2022/01/el-salvador-pegasus-spyware-surveillance-journalists/>

⁷²Legislative Assembly of the Republic of El Salvador. (June 22, 2022). *Decree No. 431. “Growing Together” Law for the Comprehensive Protection of Infants, Children, and Adolescents*. Official Gazette No. 118, Volume No. 435. <https://www.asamblea.gob.sv/node/12217>

Complementarily and reactively, strict legal protection is provided by the Special Law Against Cybercrimes and Related Offenses (Legislative Decree 260 of 2016).⁷³ This legislation devotes a specific chapter to cybercrimes against children, adolescents, and people with disabilities (Articles 24 through 27), imposing prison sentences for conduct such as the distribution and possession of child pornography, sexual blackmail through the use of information technologies, and the use of minors for the production or dissemination of explicit material via any digital device.

Furthermore, in the fight against gender-based violence in virtual environments, various criminal law reforms introduced by the Legislative Assembly have successfully established separate criminal offenses for contemporary forms of digital abuse. This has made it possible to criminalize conduct such as the non-consensual dissemination of intimate visual material (“revenge porn”), electronic sexual blackmail, and cyberbullying. However, despite the existence of this list of criminal offenses, the administration of justice faces obstacles. Limitations in digital forensic investigation, technical barriers to identifying perpetrators who operate anonymously on transnational platforms, and challenges in the speed of judicial prosecution significantly undermine the effectiveness of these laws.

4.5.6 Digital Electoral Regulation

In the area of electoral regulation, the governing rules for campaigns, financing, and campaign advertising in El Salvador are primarily contained in the Electoral Code⁷⁴ and the Political Parties Law.⁷⁵ Historically, this regulatory framework was designed to oversee analog processes and advertising in traditional mass media (television, radio, and print media). However, as the political debate has shifted to the digital sphere, this regulatory framework now suffers from a structural lag. El Salvador lacks specific regulations that criminalize modern cyber-electoral offenses or that require technology companies to transparently report the source of political advertising. This legislative omission leaves the Supreme Electoral Tribunal (TSE) without the enforcement powers and operational tools needed to monitor opaque financing—both domestic and foreign—of micro-targeted advertising on social media during election periods.

This lack of legal modernization exacerbates the vulnerability of the democratic process to algorithmic manipulation tactics. Without a legal framework that gives the TSE the “teeth” to intervene in the digital environment, the country remains exposed to cyber phenomena that are decisive in today’s democracies. Under the current framework, it is extremely difficult to investigate or curb the deployment of *bot* farms, the systematic use of inauthentic accounts, or coordinated disinformation campaigns aimed at pressuring candidates, polarizing the electorate, or suppressing voter turnout.

Paradoxically, while regulation of *online* political discourse remains stagnant, voting infrastructure has undergone significant changes. With the passage of the Special Law on Voting Abroad (Legislative Decree 541 of 2022), remote electronic voting via the internet (in addition to in-person electronic voting) was established for the vast Salvadoran diaspora. This technological leap facilitates the participation of hundreds of thousands of Salvadorans abroad, although it introduced unprecedented logistical and cybersecurity challenges. Its implementation forced the government to rely on sophisticated facial biometric validation technologies, data encryption algorithms, and international *software* providers, marking the integration of digital technology into the practice of Salvadoran democracy.

⁷³Legislative Assembly of the Republic of El Salvador. (February 4, 2016). *Decree No. 260. Special Law Against Cybercrimes and Related Offenses*. Official Gazette No. 29, Volume No. 410. <https://www.asamblea.gob.sv/node/621>

⁷⁴Legislative Assembly of the Republic of El Salvador. (July 3, 2013). *Decree No. 413. Electoral Code*. Official Gazette No. 122, Volume No. 400. <https://www.asamblea.gob.sv/node/629>

⁷⁵Legislative Assembly of the Republic of El Salvador. (January 31, 2013). *Decree No. 307. Political Parties Act*. Official Gazette No. 32, Volume No. 398. <https://www.asamblea.gob.sv/node/631>

4.6 Alignment with UNESCO Guidelines: El Salvador

An analysis of El Salvador's regulatory and institutional framework, compared with the UNESCO Guidelines for the Governance of Digital Platforms, reveals a lack of structural and practical alignment. Although the Constitution of the Republic establishes a dogmatic, rights-based framework—by protecting freedom of expression with technological neutrality (Art. 6) and enshrining the inviolability of communications (Art. 24)—the country's operational reality diverges drastically from the approach based on human rights, transparency, and due diligence promoted by the international system. In practice, El Salvador's digital ecosystem operates amid critical legal gaps and a political environment that prioritizes punitive control over multistakeholder governance.

With regard to freedom of expression and the protection of civic space, El Salvador's framework clashes head-on with the “high threshold” required by UNESCO (where restrictions must be exceptional, lawful, necessary, and proportionate). This principle has been severely violated by the imposition of a state of emergency that has been in effect continuously since March 2022, which de facto suspends the inviolability of telecommunications and legalizes unrestricted state surveillance. Added to this is the documented use of military spyware (such as Pegasus) against the press, and the promotion of criminal reforms such as the so-called “Gag Law,” which, although subsequently decriminalized, created a climate of persecution. This combination, along with the systematic operation of troll farms to stigmatize critical voices, has a profoundly chilling effect and encourages self-censorship, destroying the safe environment for public debate that UNESCO seeks to protect.

With regard to the specific governance of digital platforms, El Salvador lacks a “safe harbor” regime or a system of limited liability for internet intermediaries. In the absence of a modern law defining the role of these technology corporations, there are no incentives or legal obligations for social media platforms to establish transparent content moderation policies, assess their systemic risks, or provide due process mechanisms for users. To address this shortfall, the government resorts to punitive measures, such as the Special Law Against Cybercrimes, or applies the Consumer Protection Law on a supplementary basis to address abusive “Terms and Conditions,” overlooking the need for a comprehensive system of digital co-regulation.

Data protection and privacy represent another critical area of misalignment. El Salvador suffers from a profound structural void, as it lacks a General Law on the Protection of Personal Data applicable to the private sector, as well as an independent national authority in this area. Protection falls in a fragmented manner to the Institute for Access to Public Information (only for government data) or to case law, leaving citizens defenseless against mass data collection and commercial algorithmic profiling. Furthermore, practices in the telecommunications market—heavily rooted in prepaid plans with zero-rating schemes (data-free access to certain platforms such as Facebook or WhatsApp)—violate the principle of net neutrality, trapping users in information bubbles that limit their access to the open web and facilitate the spread of disinformation.

Finally, in the area of democratic integrity, the country faces an imbalance. On the one hand, it made a cutting-edge technological leap by enabling remote electronic voting via the internet for its diaspora through the Special Law on the Exercise of the Right to Vote Abroad (2022). On the other hand, it lags behind in enacting legislation to regulate digital campaigning. The Supreme Electoral Tribunal (TSE) lacks the authority and legal basis to audit the opaque financing of micro-targeted advertising, investigate the use of bots, or curb coordinated disinformation campaigns aimed at suppressing voter turnout. Overall, El Salvador faces the challenge of transitioning from a model of corporate surveillance and deregulation to a comprehensive digital governance framework that holds platforms accountable and restores the constitutional guarantees of the information ecosystem.

5. Country Analysis: Guatemala

5.1 Political and Legal System

Guatemala maintains a presidential system of government, and the political system operates around the three traditional branches—executive, legislative, and judicial—along with several autonomous and oversight bodies with specific constitutional functions.

The President is elected by popular vote for a four-year term, and immediate reelection is prohibited; the executive branch consists of ministries and secretariats that administer public policies, while the unicameral Congress of the Republic has the exclusive constitutional authority to introduce and process legislation. For its part, the Constitutional Court exercises both diffuse and concentrated oversight of constitutionality, and the Public Prosecutor's Office is granted the authority to conduct public criminal prosecutions.

Electoral processes are held every four years for presidential and legislative elections, which are administered by the Supreme Electoral Tribunal (TSE), which regulates candidate registration, the organization of voting, and the counting of votes; the trustworthiness and efficiency of the electoral system have been the subject of debate and reforms at various times, as will be discussed later.

The territorial organization is decentralized into departments and municipalities, which are composed of mayors and municipal councils elected by popular vote; these bodies manage municipal affairs, although effective decentralization faces financial and institutional constraints. Overall, Guatemala has formal frameworks and institutions designed to guarantee democracy and the rule of law, but a set of challenges common to the region persists, related to judicial independence, transparency, accountability, and public trust in public institutions.

5.2 Freedom of Expression and Human Rights

Guatemala expressly recognizes freedom of thought and freedom of expression in its Constitution,⁷⁶ as set forth in Articles 35 and 36, which establish not only the right of every person to disseminate their ideas without prior censorship, but also the prohibition of any indirect restriction on the exercise of this right.

These provisions are complemented by a regulatory framework that incorporates international human rights treaties into the constitutional order, in accordance with the interpretation upheld by the Constitutional Court, which has reiterated the primacy of international instruments regarding freedom of expression, information, and the press, pursuant to Articles 44 and 46 of the Constitution.⁷⁷ The country has adopted relevant legislation such as the Law on Access to Public Information (Decree 57-2008),⁷⁸ which establishes active transparency obligations and procedures to guarantee citizens'

⁷⁶National Constituent Assembly of the Republic of Guatemala. (May 31, 1985). *Political Constitution of the Republic of Guatemala*. Diario de Centro América. <https://www.cc.gob.gt/ordenamiento-juridico/constitucion-politica-de-la-republica-de-guatemala/>

⁷⁷Constitutional Court of Guatemala. (October 14, 2004). *Ruling on Case No. 1822-2003*.

⁷⁸Congress of the Republic of Guatemala. (September 23, 2008). *Law on Access to Public Information. Decree No. 57-2008*. Diario de Centro América. <https://pnc.gob.gt/wp-content/uploads/2021/04/LEY-DE-ACCESO-A-LA-INFORMACION-PUBLICA.pdf>

right to be informed about public administration, as well as electoral and media legislation, which regulate media pluralism and equity in the use of media space during electoral processes.

However, various academic studies and international organizations have pointed out that the practical effectiveness of these safeguards faces institutional and contextual challenges.⁷⁹ Among these are limitations in the application of access-to-information regulations, difficulties in ensuring the economic sustainability of independent media, and tensions between state actors and journalists that sometimes lead to a climate of mistrust or controversial legal proceedings. These situations do not represent a structural denial of these rights, guarantees, and freedoms, but they do reflect the country's need to strengthen its protection mechanisms.

Table 4. Guatemala's Scores and Rankings in Freedom of Expression Indices

Report or Index	Rating	Rank	Year
WhatsApp	40.32	138	2025
Instagram	0.81	58	2024

Source: Author's own analysis based on RSF (2025) and V-Dem (2024).

In Guatemala, judicial protection of freedom of expression and the right of access to public information is primarily provided by the Constitutional Court through the exercise of constitutional amparo, which is applicable in cases of acts or omissions that threaten or infringe upon fundamental rights. Procedural rules and constitutional doctrine govern the Court's jurisdiction to hear amparo cases either as the court of first instance or on appeal, depending on the specific case, in accordance with the provisions of the Law on Amparo, Personal Appearance, and Constitutionality (Decree 1-86)⁸⁰ and the case law of the Constitutional Court itself.

The Supreme Court of Justice also participates in the protection of constitutional guarantees by adjudicating amparo actions in the first instance or in its respective chambers; its rulings may be appealed to the Constitutional Court. In practice, the division of jurisdiction between the two courts has been clarified through joint orders and interpretive rulings issued by the Constitutional Court.

In the electoral sphere, the authority to protect rights related to freedom of expression in campaigns, access to the media, and political propaganda lies with the TSE. This body exercises jurisdictional functions regarding political rights, electoral financing, and political propaganda, as provided for in the Law on Elections and Political Parties⁸¹ and its Regulations.⁸²

At the administrative level, the Office of the Human Rights Ombudsman (PDH) acts as a supervisory and advocacy body against state acts or omissions that restrict freedom of expression or access to information. Within its structure, the PDH includes the Office for the Defense of the Right to Freedom of Expression, which is responsible for addressing complaints, issuing recommendations, and promoting protective measures for journalists and media professionals.

⁷⁹Méndez Dardón, A. M. (2022). Freedom of expression in Guatemala: between repression and resistance. *Journal of Political Science of Rafael Landívar University*, 15(2), 45–67.

⁸⁰National Constituent Assembly of the Republic of Guatemala. (January 8, 1986). *Law on Amparo, Personal Appearance, and Constitutionality. Decree No. 1-86*. Diario de Centro América. <https://www.cc.gob.gt/ordenamiento-juridico/ley-de-amparo-exhibicion-personal-y-de-constitucionalidad/>

⁸¹National Constituent Assembly of the Republic of Guatemala. (December 3, 1985). *Law on Elections and Political Parties. Decree No. 1-85*. Diario de Centro América. <https://www.tse.org.gt/index.php/leyes-y-reglamentos/ley-electoral-y-de-partidos-politicos>

⁸²Supreme Electoral Tribunal of the Republic of Guatemala. (October 12, 2016). *Regulations Governing the Electoral and Political Parties Law. Agreement No. 435-2016*. Diario de Centro América. <https://www.tse.org.gt/index.php/leyes-y-reglamentos/reglamento-a-la-lepp>

The practical implementation of the right of access to public information is governed by the Law on Access to Public Information (Decree 57-2008),⁸³ , which establishes the obligated entities, the procedures for requests and appeals, and the obligations regarding proactive transparency. Each public institution has a Public Information Unit (UIP) responsible for receiving and processing requests. Overall oversight of compliance rests with the PDH, through its Directorate of Access to Public Information.

With regard to personal data protection, Guatemala lacks comprehensive legislation and a specialized oversight authority. However, the Constitutional Court has recognized the right to privacy and the protection against misuse of data under the constitutional protection of honor and private life (Article 24 of the Political Constitution of the Republic). This regulatory situation places Guatemala behind other countries in the region in terms of informational self-determination.

In the field of telecommunications and the digital environment, the Superintendency of Telecommunications (SIT), a decentralized entity of the Ministry of Communications, Infrastructure, and Housing, is responsible for the administration of the radio spectrum, the technical and economic regulation of the sector, and the promotion of free competition in telecommunications services, in accordance with the General Telecommunications Law.⁸⁴ The SIT does not perform content moderation functions; its role is predominantly technical and supervisory with respect to the digital ecosystem's infrastructure.

Guatemala does not have a specific tax regime for digital services, but the study found that the Superintendency of Tax Administration (SAT) has implemented measures to levy Value-Added Tax (VAT) on electronic transactions and services provided via digital means under the terms of the Value-Added Tax Law,⁸⁵ , and the administrative provisions issued since 2021 regarding electronic invoicing and digital commerce.

Regarding the current state of freedoms in this area, the study found that Guatemala has a multilevel regulatory framework for protection, as this protection is legally enshrined in the Constitution, the Law on Amparo, Personal Appearance, and Constitutionality, as well as standards derived from the Inter-American Human Rights System. The Constitutional Court typically incorporates the guidelines of the Inter-American Human Rights System (SIDH) into its reasoning, particularly regarding legitimate restrictions, democratic necessity, and accountability for abuses of the right to information. However, unlike other countries such as Costa Rica, Guatemala lacks a legal framework for the protection of the right to be forgotten.

With regard to freedom of expression, Guatemalan law recognizes both the individual and collective dimensions of the right, and the forms of expression that are protected or eligible for legal protection are established by law.

In practice, by 2023, a joint mission led by Freedom House in collaboration with ARTICLE 19, the Committee to Protect Journalists (CPJ), Reporters Without Borders (RSF), Fundamedios, and Free Press Unlimited, IFEX-ALC, and Voces del Sur, conducted interviews with 67 journalists, including several in exile, to analyze the conditions under which they carry out their work in different regions of the country.⁸⁶ In its report on the findings, the mission highlights patterns of intimidation, judicial

⁸³Congress of the Republic of Guatemala. (September 23, 2008). *Law on Access to Public Information. Decree No. 57-2008*. Diario de Centro América. <https://pnc.gob.gt/wp-content/uploads/2021/04/LEY-DE-ACCESO-A-LA-INFORMACION-PUBLICA.pdf>

⁸⁴Congress of the Republic of Guatemala. (October 17, 1996). *General Telecommunications Law. Decree No. 94-96*. Diario de Centro América. <https://sit.gob.gt/gerencia-juridica/leyes-y-reglamentos/>

⁸⁵Congress of the Republic of Guatemala. (July 1, 1992). *Value-Added Tax Act. Decree No. 27-92*. Diario de Centro América. <https://portal.sat.gob.gt/portal/descarga/2026/leyes-tributarias/1546/decreto-27-92-ley-del-impuesto-al-valor-agregado.pdf>

⁸⁶ Joint mission by Freedom House, ARTICLE 19, CPJ, RSF, Free Press Unlimited, IFEX-ALC, Fundamedios, and Voces del Sur. (2023). *Report on the findings of the international mission on freedom of the press and freedom of*

persecution, and digital violence that affect both the personal safety of female journalists and the public's ability to freely access information.

According to the report, systematic harassment was observed on social media through coordinated campaigns of delegitimization or surveillance, which contributes to a climate that fosters self-censorship among those covering high-risk topics such as corruption or abuse of power.³ This document also emphasized that government agencies, such as the Office of the Human Rights Ombudsman, face difficulties in providing an adequate or effective response to threats against journalistic work and, in general, in fostering a safe environment for the free flow of information.

Additionally, the chapter on Guatemala prepared by Human Rights Watch reported at least 120 incidents of assault, harassment, and the use of criminal proceedings against journalists during the first seven months of 2023.⁸⁷ Among these incidents is the case of José Rubén Zamora, editor-in-chief of the newspaper *elPeriódico*, who was convicted of money laundering amid questions about the use of the criminal justice system to repress the press.

Furthermore, a specific report on community journalism, published by Freedom House in 2025, documents how journalists working for indigenous and local media face other types of challenges associated with factors of inequality, such as structural discrimination, gender-based violence, legal threats, and limited access to institutional protection mechanisms.⁷ These conditions seem to make it somewhat more difficult to implement the rights enshrined in the Constitution, but they also reduce these journalists' ability to report in communities with less traditional media coverage, which could be undermining media pluralism at the local level.

The reports conclude that, while guarantees and freedoms exist in a formal sense and are enforced through legal remedies, the reality on the ground reveals barriers to specific activities, such as the practice of journalism. Thus, the available data suggest that certain challenges remain to the effective exercise of the right to communicate and the right to be informed in this context.

5.3 Digital Environment

DataReportal's most recent report indicates that, as of early 2025, Guatemala had approximately 11.3 million Internet users, equivalent to a penetration rate of 60.8% of the total population⁸⁸

In terms of mobile subscriptions, consolidated data show that in 2024 there were nearly 20.65 million active cellular connections, equivalent to 113.3 connections per 100 inhabitants (this reflects the existence of multiple lines per user and a high degree of mobile connectivity).⁸⁹ Records from technical and market observatories also point to a sustained rollout of 5G: the Superintendency of Telecommunications (SIT) held spectrum auctions aimed at 5G implementation (including blocks in the 700 MHz band and other ranges designated for mobile services), and the operators that secured rights in those auctions have begun offering commercial 5G services or conducting 5G trials in urban areas, although commercial availability is still increasing gradually.⁹⁰

expression in Guatemala. <https://freedomhouse.org/sites/default/files/2023-06/Guatemala-Informe-Libertad-Expresion-2023.pdf>

⁸⁷ Human Rights Watch. (2024). *Guatemala*. In *World Report 2024*. <https://www.hrw.org/es/world-report/2024/country-chapters/guatemala>

⁸⁸ Kemp, S. (January 2025). *Digital 2025: Guatemala*. DataReportal. <https://datareportal.com/reports/digital-2025-guatemala>

⁸⁹ Kemp, S. (February 2024). *Digital 2024: Guatemala*. DataReportal. <https://datareportal.com/reports/digital-2024-guatemala> (20.65 million; 113.3 connections per 100 inhabitants).

⁹⁰ Superintendency of Telecommunications. (September 13, 2023). SIT holds 5G spectrum auction. <https://sit.gob.gt/>; see also Gamarro, U. (September 13, 2023). *5G spectrum auction completed in Guatemala*.

Mobile user experience reports (OpenSignal) show that the dominant operators offer extensive 4G coverage and that 5G performance is beginning to appear in coverage and availability metrics; in the most recent analyses, Claro and other operators rank among the providers with the highest network availability in user measurements.⁹¹

With regard to social media use, Guatemala's digital ecosystem shows widespread adoption but with distinct demographic profiles. DataReportal reported 10.4 million active social media accounts in 2025 ($\approx 56.1\%$ of the population)⁹², and its data sheets show that platforms such as TikTok reach massive audiences among users over 18 years of age⁹³; the platforms' ad planning tools reveal that TikTok and Instagram have the highest engagement among younger users (under 35), while Facebook maintains a strong presence among older age groups⁹⁴.

From a sociodemographic perspective relevant to understanding the digital ecosystem, approximately 53% of the population lives in urban areas (projected data for January 2024), which explains why most of the traffic and active users are concentrated in the country's major urban centers (Guatemala City, adjacent metropolitan areas, and the most densely populated departments).⁹⁵

In terms of tax and administrative matters related to digital platforms and services, Guatemala maintains a tax structure in which Value-Added Tax (VAT) is applied at a general rate of 12%, and the tax administration has promoted online electronic invoicing (FEL) and regulatory reforms (Decree 4-2019 and related regulations) to modernize tax collection. Although the SAT has strengthened its tools for monitoring and recording electronic transactions, unlike other countries in the region, Guatemala does not have a regime that is as explicit and differentiated—, legal, and operational—to require all non-resident providers of cross-border digital services to collect VAT from the end consumer through standardized mechanisms.

5.4 Digital Platforms Available in the Country

Guatemala does not have a public and binding registry that legally establishes the domicile of digital platforms in the country; the tax and administrative obligations applicable to them have been developed on a sector-by-sector basis and through actions by the Superintendency of Tax Administration (SAT) and other competent authorities, rather than through a single registry of platforms.⁹⁶

Prensa Libre. <https://www.prensalibre.com/economia/se-completa-subasta-de-frecuencias-para-5g-en-guatemala/>; and State News Agency (AGN), institutional coverage of the auction.

⁹¹ Analysis of 5G coverage, speed, and availability among local operators: Opensignal. (March 2025). *Guatemala: Mobile Network Experience Report March 2025*. <https://insights.opensignal.com/reports/2025/03/guatemala/mobile-network-experience>, and Opensignal. (March 2024). *Guatemala: Mobile Network Experience Report, March 2024*. <https://insights.opensignal.com/reports/2024/03/guatemala/mobile-network-experience>

⁹² Kemp, S. (January 2025). *Digital 2025: Guatemala*. DataReportal. <https://datareportal.com/reports/digital-2025-guatemala>

⁹³ Kemp, S. (February 2024). *Digital 2024: Guatemala*. DataReportal. <https://datareportal.com/reports/digital-2024-guatemala> See data on TikTok's advertising reach and distribution by gender and age for audiences 18+.

⁹⁴ StatCounter. (January 2024). *Social media stats Guatemala: Jan 2024*. <https://gs.statcounter.com/social-media-stats/all/guatemala/2024> and NapoleonCat. (January 2024). *Facebook users in Guatemala: January 2024*. <https://napoleoncat.com/stats/facebook-users-in-guatemala/2024/01/>; Platform usage statistics (market share by platform and breakdown by age group on Facebook, January 2024).

⁹⁵ Kemp, S. (February 2024). *Digital 2024: Guatemala*. DataReportal. <https://datareportal.com/reports/digital-2024-guatemala> See total population and urban percentage, January 2024.

⁹⁶ Vesco Consultores. (May 8, 2024). *Taxation of Digital Platforms in Guatemala*. <https://vescco.tax/blog/tributacion-de-las-plataformas-digitales-en-guatemala/>; Meléndez, O. (2022). *Taxation in*

Table 5. Distribution of Users by Digital Platform in Guatemala

Platform	Number of users (in millions)
WhatsApp	7.21
Instagram	3.40
TikTok	9.11
Facebook	8.60
YouTube	7.34
Twitter (X)	0.96

Source: Compiled by the author based on DataReportal and SensorTower⁹⁷

Regarding political campaigns, the Supreme Electoral Tribunal has the Specialized Unit on Media and Opinion Polls (UEMCEO), which provides training to political parties on the authorized uses of advertising on social media. Another detail is that a reform passed in 2022 established that political organizations must register with the Unit a single page for the political party, verified by the social media platform on which they have duly posted the disclaimer, in the manner and within the timeframe required by the platform, such that they may only make payments to digital platforms for content published on those reported and verified sites.

5.5. Legislative and Regulatory Context in Guatemala

5.5.1 Constitutional Framework

The Guatemalan constitutional framework expressly sets forth principles and rights related to freedoms and guarantees for expression, information, and communications. Structurally, the constitutional system provides for centralized oversight of constitutionality through the Constitutional Court, an institution that acts as the central body for the protection of these fundamental rights; it is to this court that amparo petitions related to violations of access to information and freedom of expression are typically filed.

Likewise, the constitutional framework assigns distinct powers to State bodies with respect to communications and telecommunications. The ordinary legislature retains broad discretion to define the scope of freedom of expression and the media regime, while the Executive Branch retains administrative authority over the radio spectrum.

This regulatory framework governs any intervention regarding digital content or platform-specific dynamics, requiring compliance with the constitutional limits established in the case law of the Constitutional Court. That Court has reiterated the principles of the Inter-American system regarding proportionality and the prohibition of indirect restrictions.

the Digital Economy in Guatemala. Universidad del Istmo. <https://unis.edu.gt/wp-content/uploads/2022/08/Articulo-2.-Lcda.-Olga-Melendez.-Final.pdf>

⁹⁷Sensor Tower. (September 2024). *Top social networking apps in Guatemala, Q3 2024: Unified platform*. <https://sensortower.com/blog/2024-q3-unified-top-5-social%20networking-units-gt-600b30a6241bc16eb80bb51d>

5.5.2 Telecommunications and Media Legislation

Guatemala's legal framework for telecommunications is based primarily on the General Telecommunications Law (Decree 94-96), which establishes a technical and economic regime for the use of the radio spectrum and the provision of communications services, similar to the systems currently in place in other countries in the region.⁹⁸

Under this law, the country established the Superintendency of Telecommunications (SIT) as a technically independent agency attached to the Ministry of Communications, empowered to administer the telecommunications registry, oversee spectrum use, plan national numbering, and resolve disputes among operators regarding access to essential resources.⁹⁹ By law, the SIT is involved in the oversight of operators, but its primary focus is on technical and operational matters rather than on regulating online content or speech.

Additionally, the Freedom of Expression Act¹⁰⁰ prohibits prior censorship and the requirement of a security deposit for publication, and it also establishes liability for defamation or slander after the fact.⁶ A notable feature is that this law established a Court of Honor as a mechanism for resolving disputes between public officials and the media

Initiatives have been proposed in the country to regulate other aspects, such as the Personal Data Protection Bill (¹⁰¹), which as of 2025 was still pending legislative action. Its purpose is to protect personal data using standards inspired by the European Union's General Data Protection Regulation (GDPR), as well as to create an independent authority with the power to impose sanctions.

5.5.3 Specific Regulation of Platforms and/or Content

Like other countries covered in this study, Guatemala does not have a legal framework regulating digital platforms as service providers or content intermediaries. Platform activity falls under general provisions on e-commerce, consumer protection, intellectual property, and civil liability, but there are no specific regulations on content moderation, reporting obligations, or algorithmic transparency.

In the electoral sphere, the Supreme Electoral Tribunal (TSE) has issued administrative provisions to limit or channel political advertising on social media during specific periods, but these rules have varied throughout electoral processes and are based on the interpretation of Article 223 of the Electoral and Political Parties Law (LEPP).¹⁰² The absence of specialized legislation appears to create a scenario in which decisions regarding digital content are made through regulatory or administrative powers, subject to constitutional review, as is the case with the imposition of VAT on digital platforms.

⁹⁸Congress of the Republic of Guatemala. (October 18, 1996). *General Telecommunications Law [Decree No. 94-96]*. Official Gazettes of Central America.

⁹⁹Congress of the Republic of Guatemala. (October 18, 1996). *General Telecommunications Law [Decree No. 94-96]*. Official Gazettes of Central America. Articles 5–7 establish the creation, functions, and powers of the Superintendency of Telecommunications.

¹⁰⁰National Constituent Assembly of the Republic of Guatemala. (May 5, 1966). Law on Freedom of Expression [Decree No. 9]. *Diario de Centro América*. https://www.congreso.gob.gt/assets/uploads/congreso/marco_legal/7c326-ley-de-emision-del-pensamiento.pdf

¹⁰¹Congress of the Republic of Guatemala. (July 8, 2025). Bill to Approve the Personal Data Protection Act [Bill No. 6572]. Legislative Directorate. Article 1 establishes that the purpose of the law is to strengthen the constitutional guarantee of the right to privacy and the protection of every person's data. https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/1c48c-6572.pdf

¹⁰²National Constituent Assembly of the Republic of Guatemala. (December 3, 1985). *Electoral and Political Parties Law [Decree No. 1-85]*.

5.5.4 Legislation on Data Protection and Privacy

Guatemala has not adopted a general law on personal data protection. Existing regulations are scattered across sector-specific laws such as the Law on Access to Public Information (Decree 57-2008),¹⁰³ which defines categories of sensitive personal information and establishes the obligation to safeguard data held by public entities. There are also isolated provisions in banking, financial, and healthcare legislation that regulate the processing of information under specific regimes.

The absence of a national data protection authority limits the institutional capacity to oversee digital operators, platforms, or private entities that manage personal information. Consequently, the privacy framework operates primarily on the basis of constitutional principles, civil liability, and judicial review through amparo proceedings, which leaves significant gaps regarding digital rights and automated data processing.

5.5.5 Specific Regulations for the Protection of Vulnerable Groups

The protection of vulnerable populations in the digital environment is scattered across various sector-specific regulations, without a unified framework; thus, their protection is provided for in provisions such as the Comprehensive Protection of Children and Adolescents Act (Decree 27-2003) and the Act on the Prevention and Punishment of Crimes Against Women and Children (¹⁰⁴), which established obligations regarding prevention and punishment in cases of exploitation, abuse, or misuse of images and data of minors. This clearly impacts the handling of digital content. With regard to violence against women, the Law Against Femicide and Other Forms of Violence Against Women also incorporated provisions that can be extended to conduct carried out through information technologies or digital media.

In the absence of a specific regulatory framework for digital risks, the application of these standards depends on the specific case and on institutional capacity to identify impacts arising from the platform ecosystem. The regulatory approach remains predominantly focused on criminal law and personal protection, rather than a preventive framework for digital governance.

5.5.6 Digital Electoral Regulation

Guatemala's electoral regulatory framework is governed by the Electoral and Political Parties Law (LEPP), which currently regulates public and private party financing, as well as obligations regarding electoral advertising in traditional media.¹⁰⁵ In particular, Article 222 of the law stipulates that during election periods, political organizations may not contract for campaign advertising directly with media outlets; rather, the TSE must centralize these media slots and set rates.¹⁰⁶ Likewise, Article 223 establishes prohibitions on campaign advertising, although it does not explicitly classify paid digital advertising as part of those restrictions.

Since current regulations did not provide a clear, specific framework for contracting paid advertisements on digital platforms, the TSE has relied on internal agreements and regulations to fill

¹⁰³Congress of the Republic of Guatemala. (October 23, 2008). Law on Access to Public Information [Decree No. 57-2008]. *Diario de Centro América*.

¹⁰⁴Congress of the Republic of Guatemala. (July 18, 2003). Comprehensive Protection of Children and Adolescents Act [Decree No. 27-2003]. *Diario de Centro América*. <https://www.albakeneth.gob.gt/public/leyes/LeyProteccionIntegraldeLaNinezyAdolescencia.pdf>

¹⁰⁵ National Constituent Assembly. (1985). *Law on Elections and Political Parties* [Decree No. 1-85]. Official Gazettes of Central America, Articles 222 and 223.

¹⁰⁶Supreme Electoral Tribunal. (January 19, 2018). *Regulations of the Specialized Unit on Media and Public Opinion Polls* [Agreement No. 15-2018], Article 2 Bis, definition of "media": includes "social media and digital media via the Internet."

that gap. For example, the Regulations of the Specialized Unit on Media and Opinion Polls (UEMCEO) include “social media and digital media via the internet” in its definition of media for the purposes of monitoring and political advertising. These regulations require those who intend to advertise on social media to first register their political accounts with the TSE, which allows for some institutional control over paid advertisements. However, this measure may be leaving content posted from other, unreported accounts unchecked.

The TSE has clarified that political parties may only run ads on certain platforms (Facebook, Instagram, WhatsApp) and only after formal registration and verification by the electoral body.

The challenge facing the country in this area is the tension between traditional media regulation and the need to adapt to election campaigns conducted digitally. While it is true that the LEPP did not explicitly address all aspects of political advertising on social media, the TSE has responded with regulatory and operational reforms to address this legislative omission.

5.6 Alignment with UNESCO Guidelines: Guatemala

The Guatemalan constitutional framework establishes a set of guarantees aimed at protecting freedom of expression, prohibiting prior censorship, and ensuring the inviolability of correspondence and communications. Although this regulatory framework lays the groundwork required by international human rights standards, the country faces challenges because it has not incorporated recent reforms regarding technology-related rights, access to telecommunications, or comprehensive protection of personal data.

Despite having regulatory tools such as the Law on Access to Public Information and the Law on Freedom of Expression, the legal system lacks specific legal mechanisms to require transparency from digital platforms, audit automated systems, or ensure a balance in the face of potential violations of users' rights. Furthermore, while the Constitutional Court applies criteria of legality, necessity, and proportionality when reviewing potential restrictions on fundamental rights, these safeguards operate primarily in a reactive manner through *ex post* judicial review, as is the case with the amparo proceeding. This contrasts with global guidelines that suggest integrating these tests into prior, verifiable administrative procedures specifically aimed at moderating digital content.

This lack of a preventive and unified approach is reflected in a markedly fragmented regulatory landscape. Current legislation treats telecommunications, access to information, traditional media, and electoral matters separately, with no comprehensive law defining the regulatory scope for digital platforms as intermediaries. Consequently, the country lacks a structured liability regime for these technology companies that includes clear obligations regarding content moderation, algorithmic transparency, respect for due process for users, or due diligence.

Government interventions in this area tend to be purely sector-specific, which disperses oversight across multiple public entities with differing procedures. For example, while there are robust administrative regulations governing the allocation of the electromagnetic spectrum, in the digital sphere it is the Supreme Electoral Tribunal (TSE) that has had to rely on agreements and regulatory guidelines to monitor social media, manage campaign advertising, and combat disinformation during elections. However, these valuable electoral efforts lack higher-level legal backing and fail to impose mandatory structural processes on platforms, such as independent audits or internal appeal systems.

In practice, the absence of a systemic framework directly impacts the protection of specific segments of the population and the free exercise of journalism. Although the Constitution expressly prohibits arbitrary state intervention regarding content, various independent reports have highlighted incidents where the use of criminal and administrative measures has sparked public debate due to their alleged negative impact on freedom of the press and expression.

On the other hand, regarding vulnerable populations, Guatemala has protective laws focused on children, adolescents, and women, which are applicable to behavior in the online environment; however, these regulations do not translate into concrete obligations for platforms to proactively mitigate risks or establish priority and specialized reporting channels.

Finally, regarding citizen empowerment, the country has taken enabling steps such as the legal recognition of digital identity through electronic signatures and the promotion of a culture of transparency. However, there remains a gap in robust national policies on media and digital literacy that actively equip the population to critically evaluate content, identify disinformation campaigns, and understand the algorithmic systems with which they interact on a daily basis.

6. Country Analysis: Honduras

6.1 Political and Legal System

Honduras' regulatory and political framework is based on its 1982 Constitution¹⁰⁷ (with its respective amendments), which defines the country as a free, democratic, sovereign, and independent republic (Art. 1). Its form of government is republican, democratic, and representative, based on the inalienable principle that sovereignty resides essentially in the people, from whom all powers of the State emanate (Art. 2). The exercise of public power is structured under a system of separation of powers, which are complementary, independent, and not subordinate to one another: the Legislative Branch, exercised by the National Congress; the Executive Branch, headed by the Presidency of the Republic; and the Judicial Branch, whose highest authority is the Supreme Court of Justice (Art. 4).

In the political-electoral sphere, the Honduran legal system recently underwent a profound institutional restructuring aimed at strengthening the transparency and integrity of elections. This reform separated administrative functions from judicial ones, eliminating the former Supreme Electoral Tribunal to make way for two specialized bodies. On the one hand, the National Electoral Council (CNE) was established, an autonomous entity responsible for the organization, management, and technical and administrative oversight of elections. On the other hand, the Electoral Court of Justice (TJE) was created, established as the highest judicial authority to resolve disputes in this area. This new democratic framework was legally consolidated with the enactment of the Electoral Law of Honduras (Decree 35-2021)¹⁰⁸, which regulates the functioning of the CNE and sets forth the governing rules of the electoral process.

Beyond the three traditional branches of government, the institutional design of the Honduran state includes a series of oversight bodies and decentralized entities that are fundamental to the protection of citizens' rights. The specific protection of fundamental rights falls constitutionally to the National Human Rights Commissioner (CONADEH), created under Article 59 of the Constitution with the mandate to ensure respect for human rights and to protect citizens against abuses of public power. Additionally, oversight of state resources is supervised by the Superior Court of Accounts.

Finally, this institutional framework is complemented by entities of vital importance for the governance of the country's communications and digital environment. Among these are the Institute for Access to Public Information (IAIP), the body that guarantees the right to know and government transparency (Law on Transparency and Access to Public Information), and the National Telecommunications Commission (CONATEL), the regulatory body responsible for managing the radio spectrum, granting concessions, and coordinating telecommunications and internet regulations throughout the country. Together, these bodies constitute the administrative and institutional framework within which human rights policies, technology regulation, and public deliberation are debated in Honduras.

6.2 Freedom of Expression and Human Rights

¹⁰⁷National Constituent Assembly. (January 20, 1982). *Constitution of the Republic of Honduras* [Decree No. 131]. La Gaceta. https://www.tsc.gob.hn/web/leyes/Constitucion_de_la_Republica.pdf

¹⁰⁸National Congress of Honduras. (May 26, 2021). Electoral Law of Honduras [Decree No. 35-2021]. La Gaceta. <https://www.tsc.gob.hn/web/leyes/Ley-Electoral-Honduras-2021.pdf>

The Honduran Constitution guarantees the free expression of thought through any medium of communication without prior censorship (Art. 72), although with exceptions, as prior censorship may be established by law “to protect the ethical and cultural values of society, as well as the rights of individuals,” particularly children, adolescents, and youth (Art. 75).

It is established that the management of the media and its “intellectual, political, and administrative orientation” must be exercised exclusively by Hondurans by birth (Art. 73). The same article stipulates that printing facilities and media outlets may not be seized or shut down for offenses related to the expression of ideas, and Article 74 states that the right to express ideas may not be restricted through indirect means, including the abuse of official or private controls over the media used to disseminate information.

Article 76 of the Constitution guarantees the right to honor, personal and family privacy, and one’s own image—all of which place limits on freedom of expression. Article 77 establishes freedom of worship “provided it does not contravene the laws and public order,” but prohibits ministers of various religions from engaging in any form of public propaganda. The freedoms of association and assembly are guaranteed “provided they are not contrary to public order and public morals” (Article 78), as are the freedoms of demonstration and assembly (Article 79); however, the same article provides that “outdoor gatherings and those of a political nature may be subject to a special permit system for the sole purpose of ensuring public order.” Article 80 establishes the right to petition.

Article 100 establishes the inviolability and confidentiality of communications, except by court order, and Article 182 establishes a right to Habeas Data, which includes the right of individuals to access information about themselves contained in databases and public or private records, as well as the rights to update, rectify, or amend such information. Although these rights related to data protection are mentioned, the country lacks specific legislation on the matter.

Despite the guarantees contained in the Honduran Constitution, challenges persist. International reports highlight risks to press freedom, including intimidation and violence against journalists. According to Reporters Without Borders, Honduras ranks 142nd out of 180 with a score of 38.51, a slight improvement over the previous year.¹⁰⁹

Another challenge highlighted by this organization is the acquisition of major media outlets by international investors and of smaller outlets by the local political class, compounded by the fact that other media outlets were already owned by religious entities and other businesspeople, which jeopardizes media pluralism in a country where, according to the report, “bias in reporting is palpable.” Independent journalism is also threatened by dependence on government advertising and the excessive use by officials of the right of reply. Journalists also face difficulties in accessing sources of information that are not aligned with the government.

The Penal Code has been the subject of debate for retaining provisions that could criminalize speech. Although efforts have been made to decriminalize defamation in favor of civil proceedings, insult and slander remain criminal offenses with penalties that may include imprisonment or fines; furthermore, journalists can still be prosecuted for defamation, and in some cases, convictions are accompanied by professional disqualification. The Penal Code¹¹⁰, in effect since 2020, also criminalizes demonstrations and assemblies and opens the door to the imposition of fines not only on journalists but also on those who reproduce their writings, thereby jeopardizing the right to freely seek, receive, and impart ideas and opinions, as provided for in international treaties.

The privacy of communications is inviolable (Art. 100 of the Constitution) and may only be intercepted by court order. Despite this, the Special Law on the Interception of Private Communications (Decree

¹⁰⁹Reporters Without Borders. (n.d.). *Honduras*. <https://rsf.org/es/pais/honduras>

¹¹⁰National Congress of Honduras. (October 18, 2017). *Penal Code of Honduras [Decree No. 130-2017]*. La Gaceta. https://www.tsc.gob.hn/web/leyes/Decreto_130-2017.pdf

243-2011)¹¹¹ —which regulates this procedure for criminal investigations and established the Communications Interception Unit (UIC)—has raised particular concern. Critics argue that it facilitates police wiretapping of citizens without adequate safeguards, thereby jeopardizing people's privacy.¹¹² RSF also reports that this situation has intensified in the run-up to the 2025 presidential elections.¹¹³

Organizations such as Derechos Digitales have reported that all major political parties in the country use bots to influence the vote. There is also a clear presence of fake news sites with a clear bias in favor of one party or another, and the use of social media to spread manipulation and disinformation campaigns is common.¹¹⁴

6.3 Digital Environment

Honduras is showing growth in connectivity, although a significant digital divide persists. The Honduran government's own Digital Government Plan notes that the country lags behind in e-government indicators (ranked 155th on the 2022 UN index).

According to recent data (2024), internet penetration stands at around 65.9% (Honduras Verifica), with approximately 7 million active users (DIGER). Mobile connectivity exceeds 8 million connections and is the primary means of access.

The connectivity landscape in Honduras is also heavily influenced by the structure of its telecommunications market and limitations in the quality of available infrastructure. The mobile services sector is highly concentrated, historically dominated by two large transnational companies (Tigo and Claro), which has limited competition and kept data plan costs relatively high in proportion to the population's per capita income.

In addition, according to international measurements from Ookla's Speedtest Global Index (2024), the country typically ranks among the lowest in Latin America in terms of average connection speeds, for both fixed and mobile broadband. This combination of high costs and poor speeds forces the vast majority of users to rely almost exclusively on prepaid plans and zero-rating practices (which offer "free" or unlimited access to specific social media platforms such as WhatsApp or Facebook).

While such a dynamic facilitates a basic level of communication, it fragments the browsing experience, effectively undermines the principle of net neutrality, and confines citizens to limited information ecosystems—which exacerbates their vulnerability to misinformation by making it difficult for them to access the open web to cross-check sources or verify news.

6.4 Digital Platforms Available in the Country

¹¹¹National Congress of Honduras. (December 12, 2011). *Special Law on the Interception of Private Communications* [Decree No. 243-2011]. La Gaceta. <https://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Especial%20sobre%20Intervencion%20de%20las%20Comunicaciones%20Privadas.pdf>

¹¹²Movimiento Puente. (n.d.). *Honduras: Digital Rights*. <https://derechosdigitales.movpuente.com/honduras/>

¹¹³Reporters Without Borders. (May 22, 2023). *Honduras: RSF and seven partner organizations denounce a climate of surveillance, intimidation, and violence against the press*. <https://rsf.org/es/honduras-rsf-y-siete-organizaciones-asociadas-denuncian-un-clima-de-vigilancia-intimidaci%C3%B3n-y>

¹¹⁴Movimiento Puente. (n.d.). *Honduras: Electoral disinformation*. <https://derechosdigitales.movpuente.com/desinformacion-electoral/>

As for social media, there are an estimated 4.55 million active users as of early 2024, with a strong presence of platforms such as TikTok, Facebook, Instagram, and YouTube. TikTok has positioned itself as one of the fastest-growing platforms with the widest reach.¹¹⁵

In Honduras, there are 4.39 million social media users, of whom 52.9% are women and 47.1% are men.¹¹⁶ The most widely used social media platforms are TikTok, Facebook, YouTube, Instagram, and LinkedIn. These platforms are widely used for both personal communication and the dissemination of information and political propaganda. Advertising campaigns typically use Messenger (also owned by Meta, like Facebook and Instagram), TikTok, and Facebook itself.¹¹⁷

6.5 Legislative and Regulatory Context in Honduras

6.5.1 Constitutional Framework

The Constitution of the Republic of Honduras lays the fundamental groundwork for the exercise of freedom of expression and freedom of the press—rights that today face the challenge of being applied in a balanced manner within the digital ecosystem. Article 72 guarantees that “the expression of thought through any medium of dissemination is free, without prior censorship.” This open and technologically neutral wording naturally extends constitutional protection to digital platforms and social media. Likewise, Article 73 establishes strong substantive protection by prohibiting the seizure, confiscation, or closure of media outlets, their assets, or infrastructure on the grounds of offenses related to the expression of thought. In turn, Article 74 prevents the indirect restriction of these freedoms through abusive state controls. Furthermore, privacy and informational self-determination are safeguarded by Article 182, which enshrines the right to *Habeas Data*—a vital guarantee in the context of data collection by technology platforms.

However, the constitutional framework contains exceptions that pose a challenge for online environments: Article 75 establishes that the law may impose prior censorship in order to “protect the ethical and cultural values of society, as well as the rights of individuals, especially children, adolescents, and young people.” This clause, due to the breadth and ambiguity of its moral terms, poses a latent risk to digital governance, as it could be used to justify internet content blocks, filters, or restrictions based on discretionary criteria, thereby undermining freedom of expression.

6.5.2 Telecommunications and Media Legislation

The telecommunications and media sector in Honduras is regulated by the Framework Law for the Telecommunications Sector, enacted by Decree 185-95.¹¹⁸ This legislation comprehensively regulates services and the administration of the radio spectrum and establishes the National

¹¹⁵La Prensa. (February 21, 2024). *Honduras Reaches 4.5 Million Social Media Users in 2024*. <https://www.laprensa.hn/honduras/honduras-usuarios-redes-sociales-2024-tiktok-facebook-digital-kemp-BA17616235>

¹¹⁶Shum, Y. (February 16, 2023). *Digital Landscape, Internet, and Social Media in Honduras 2023*. <https://yiminshum.com/estadisticas-digital-internet-redes-sociales-honduras-2023/>

¹¹⁷Kemp, S. (February 2024). *Digital 2024: Honduras*. DataReportal. <https://datareportal.com/reports/digital-2024-honduras>

¹¹⁸National Congress of Honduras. (October 31, 1995). *Framework Law on the Telecommunications Sector* [Decree No. 185-95]. La Gaceta. https://www.conatel.gob.hn/transparencia/leyes/Ley_Marco_Sector_Telecomunicaciones.pdf

Telecommunications Commission (CONATEL) as the sector's supreme regulatory body. The law establishes a clear taxonomy, classifying services into carrier, end-user, value-added, and broadcasting services. This regulatory framework is complemented and implemented through the General Regulations of the Framework Law, which elaborates on this classification of services in depth and outlines CONATEL's specific powers.

With regard to freedom of expression and the press, Honduras is governed by the Law on the Expression of Thought (¹¹⁹), a 1958 statute that remains in force in all respects that do not contravene the country's current Constitution.

Article 2 of that law reaffirms the fundamental right to investigate, receive, and disseminate information through any means of expression. In accordance with constitutional provisions, the law establishes substantive safeguards (Article 3) and provides legal protection for journalists, safeguarding them even during states of siege (Article 4).

However, the Honduran regulatory framework presents clear tensions with modern human rights standards. For example, Article 6 explicitly prohibits the circulation of publications that "preach subversive doctrines that undermine the foundations of the State or the family," a highly ambiguous formulation. Additionally, the law maintains anachronistic controls, such as the prohibition on the use of pseudonyms in publications (Article 26) and the ban on foreigners from directing media outlets (Article 30).

6.5.3 Specific Regulation of Platforms and/or Content Regulation

Honduras' legal framework currently lacks specific and comprehensive legislation designed to regulate social media platforms. Therefore, the most direct legal instrument governing the provision of online services is the Regulation on Internet Service or Access to Computer Networks.¹²⁰ This regulation designates internet access as a priority public service of great national interest, formally classifying it within the category of "value-added service." Its main objective is to ensure that the provision of this service is efficient, continuous, and uninterrupted, by establishing the technical requirements, the use of protocols, and the general regulations that internet service providers (ISPs) must strictly comply with in order to operate within Honduran territory.

A key feature of this regulation is the breadth with which it defines the scope and modalities of the network to adapt to the digital environment. According to Article 11 of the regulations, internet services extend far beyond traditional web browsing, explicitly including within their regulatory scope "multimedia and hypermedia content applications, animations, and online video" and, more generally, "Information Society Services."

To sustain this ecosystem, the law requires companies to operate under free competition and guarantee high-quality connectivity at affordable rates. As a control mechanism, operators must measure and report specific technical parameters to CONATEL every six months, such as connection speed (bandwidth), latency, and data packet loss.

In the area of content protection and control, the regulations impose specific obligations on both providers and end users. At the technical level, they require ISPs to implement hardware and software systems to protect network integrity and restrict spam.

¹¹⁹National Constituent Assembly. (July 26, 1958). Law on Freedom of Expression [Decree No. 6]. La Gaceta. <https://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20de%20Emision%20del%20Pensamiento.pdf>

¹²⁰National Telecommunications Commission. (August 23, 2011). *Regulations on Internet Service or Access to Computer Networks* [Resolution No. NR004/11]. La Gaceta. https://www.conatel.gob.hn/transparencia/reglamentos/Reglamento_Servicio_Internet_Acceso_Redes_Informaticas.pdf

At the user level, Article 30(b) expressly prohibits “illegal and/or immoral activities” that violate public decency, while Article 38(c) prohibits the use of the infrastructure to spread viruses, send spam, or post defamatory or slanderous messages. However, amid these prohibitions, it is vital to note that the Honduran legal framework lacks a clear legal framework for liability exemptions that would protect platforms from user-generated content.

Finally, beyond the technical, operational, and behavioral control provisions, the regulation stands out for its focus on inclusion and bridging the digital divide. The law incorporates guidelines for the universalization of services through the social cooperation program “El Internet de Todos—Conexión al Mundo” (The Internet for All—Connection to the World).¹²¹ Under this mandate, telecommunications operators are required to contribute to the country by providing free internet access in rural, urban-marginal, and historically underserved areas. With this social impact measure, the Honduran government seeks to ensure that technological expansion and access to information benefit all of society equitably, thereby promoting the educational, social, and economic development of the most vulnerable populations.

In the commercial sphere, the Law on Electronic Signatures¹²² grants legal validity to data messages and electronic signatures. Complementarily, the Consumer Protection Law¹²³ addresses virtual environments and is a pioneer in the treatment of adhesion contracts or “Terms and Conditions.” Article 69 declares null and void any unfair terms that restrict consumer rights or allow a company to unilaterally modify the contract.

6.5.4 Data Protection and Privacy Legislation

Within the Honduran legal framework, there is no General Law on the Protection of Personal Data applicable to the private sector, nor is there a specialized supervisory authority. However, the human right to *Habeas Data*, enshrined in Article 182 of the Constitution, empowers citizens to access, update, and correct inaccurate personal information in public or private databases.

In the public administration, the Law on Transparency and Access to Public Information (Decree 170-2006)¹²⁴ protects confidential data held by the State, with the Institute for Access to Public Information (IAIP) serving as the guarantor of this protection.

It is worth reiterating that the State enacted a Special Law on the Interception of Private Communications, which, as previously mentioned, regulates the procedures—under a court order—for intercepting digital communications in the prosecution of crimes.

6.5.5 Specific Regulations for the Protection of Vulnerable Groups

Although Honduras does not have a law dedicated exclusively to digital violence or the digital rights of vulnerable groups, there are sector-specific regulations that address these risks.

¹²¹Government of the Republic of Honduras. (2022). *Social Cooperation Program “The Internet for All—Connection to the World.”* Secretariat of State for Social Development.

¹²²National Congress of Honduras. (December 11, 2013). *Law on Electronic Signatures [Decree No. 149-2013]*. La Gaceta. https://www.sefin.gob.hn/wp-content/uploads/2020/11/Ley_firmas_electronicas_2013.pdf

¹²³National Congress of Honduras. (July 7, 2008). *Consumer Protection Act [Decree No. 24-2008]*. La Gaceta. <https://www.tsc.gob.hn/web/leyes/Ley%20de%20Protecci%C3%B3n%20al%20Consumidor.pdf>

¹²⁴National Congress of Honduras. (December 30, 2006). *Law on Transparency and Access to Public Information [Decree No. 170-2006]*. La Gaceta. <https://www.iaip.gob.hn/wp-content/uploads/2016/11/Ley-de-Transparencia-y-Acceso-a-la-Informacion-Publica.pdf>

The Internet Service Regulations¹²⁵ contain provisions to combat online exploitation: Article 38(e) expressly prohibits the creation or distribution of obscene material and categorically bans the reproduction or distribution of child pornography over networks. For its part, the Consumer Protection Law safeguards human dignity by prohibiting advertising or actions that undermine the honor or image of users (Article 20) and by requiring fair and dignified treatment (Article 67).

6.5.6 Digital Electoral Regulation

Honduras' democratic ecosystem has modernized its mechanisms through the Honduran Electoral Law (Decree 35-2021).¹²⁶ This law regulates campaign advertising by subjecting digital platforms to the same time and content restrictions as traditional media, and penalizes "anonymous campaigning" in the media, seeking to prevent covert campaigns.

Honduran legislation does not specifically define cyber electoral crimes; instead, Article 310 of the Electoral Law expressly states that the ordinary courts are responsible for adjudicating crimes committed during elections, with the general criminal law defining such offenses and imposing penalties. Disputes over campaign violations on digital platforms fall under the supervision of the National Electoral Council (CNE).

6.6 Alignment with the UNESCO Guidelines: Honduras

An analysis of Honduras' regulatory and institutional framework, compared with the UNESCO Guidelines for the Governance of Digital Platforms, reveals an ecosystem with structural gaps and a significant regulatory lag.

Although the Constitution of the Republic establishes a theoretical foundation for the protection of rights by prohibiting prior censorship and enshrining the inviolability of communications and the *right to data protection* (*Habeas Data*), the practical application of these rights in the digital environment is hampered by anachronistic regulations, legal loopholes, and an institutional design that is inconsistent with the *multistakeholder* approach and human rights due diligence promoted at the international level.

Regarding freedom of expression and content restrictions, the Honduran regulatory framework shows clear tensions with the "high threshold" required by UNESCO (based on the principles of legality, necessity, and proportionality). On the one hand, the Constitution itself, in Article 75, opens the door to prior censorship under broad and ambiguous justifications such as the protection of "ethical and cultural values." On the other hand, the continued existence of the 1958 Law on the Expression of Thought maintains prohibitions incompatible with modern standards, such as the ban on the use of pseudonyms—which directly contravenes the international defense of online anonymity to protect dissident voices and journalists—and the censorship of "subversive doctrines." Furthermore, the persistence of crimes against honor (insult and defamation) in the Penal Code creates a severe deterrent effect on public debate and journalism on social media, running counter to UNESCO's recommendation to decriminalize such expression.

With regard to the specific governance of digital platforms, Honduras lacks legal incentives for platforms to establish transparent, fair, and predictable mechanisms for content moderation and user

¹²⁵National Telecommunications Commission. (August 23, 2011). *Regulations on Internet Service or Access to Computer Networks* [Resolution No. NR004/11]. La Gaceta. https://www.conatel.gob.hn/transparencia/reglamentos/Reglamento_Servicio_Internet_Acceso_Redes_Informaticas.pdf

¹²⁶National Congress of Honduras. (May 26, 2021). *Electoral Law of Honduras* [Decree No. 35-2021]. La Gaceta (No. 35,609). <https://www.tsc.gob.hn/web/leyes/Ley-Electoral-Honduras-2021.pdf>

appeals. Instead, online conduct is regulated on a sector-by-sector basis through CONATEL's Internet Service Regulations, which impose extremely vague prohibitions on users—such as refraining from engaging in “immoral” activities or those contrary to “public decency”—that facilitate arbitrariness and lack the analytical rigor required by international human rights law.

Data protection and institutional design represent another critical area of misalignment. Honduras lacks a General Law on the Protection of Personal Data applicable to the private sector, as well as an independent National Data Protection Authority. Tolerated commercial practices, such as *zero-rating* (“free” access to certain social media platforms), undermine net neutrality and trap users in information bubbles, making it difficult to verify information on the open web and fueling the spread of misinformation. Added to this are legitimate concerns about the Special Law on the Interception of Private Communications, which lacks robust checks and balances against state surveillance.

Finally, in the area of democratic integrity, the country has taken steps to adapt its legislation through the 2021 Electoral Law, which subjects digital advertising to the same rules regarding timing and content as traditional media and prohibits “anonymous propaganda” to mitigate the use of *bot* farms and fake accounts. However, these measures focus on penalizing political actors and local users, but do not impose statutory obligations regarding transparency, systemic risk assessment, or accountability on the platforms themselves. Overall, Honduras faces the enormous challenge of transitioning from a fragmented, punitive, and analog regulatory ecosystem to a comprehensive digital governance framework that empowers users and requires technology companies to exercise due diligence without compromising the country's fragile state of press freedom.

7. Country Analysis: Mexico

7.1 Political and Legal System

Mexico is a federal republic governed by the 1917 Constitution¹²⁷, which establishes a presidential political system. Executive power rests with the President of the Republic, who is elected by direct universal suffrage for a six-year term without the possibility of reelection, and is supported by a cabinet composed of 19 ministries.

At the territorial level, the country is organized into 32 autonomous federal entities (31 states and Mexico City), which are subdivided into 2,469 municipalities—known as “alcaldías” in the capital—and smaller localities, whether rural or urban. Federal legislative power resides in the Congress of the Union, a bicameral body with broad powers, such as directing foreign policy and confirming high-level appointments. It is composed of the Chamber of Deputies (500 members elected every three years) and the Senate (128 members elected for six-year terms), with both chambers combining the principles of relative majority and proportional representation and allowing for limited consecutive reelection.

For its part, the judicial branch is headed by the Supreme Court of Justice of the Nation (SCJN), the country’s highest court, composed of eleven justices who sit as a full bench and in two chambers to hear constitutional, criminal, civil, labor, and administrative cases.

Finally, this system of separation of powers is replicated at the local level due to the dual nature of Mexico’s legal and administrative systems. Each state has a governor who exercises executive power for a non-renewable six-year term, a unicameral state legislature, and its own Superior Court of Justice, which enforces the relevant local legislation. Likewise, municipal councils, which form the basis of local government, are generally elected for three-year terms, with the legal possibility of reelection in accordance with the provisions of the federal Constitution and the constitution of each state.

Beginning in December 2024, a process of structural changes to various Mexican government institutions began, during which far-reaching legislative and constitutional reforms have been promoted that affect key areas such as transparency, personal data protection, economic competition, and telecommunications. A central pillar of this process is the so-called constitutional reform on organizational simplification, which was published on December 20, 2024. This reform amended various articles of the Political Constitution of the United Mexican States (CPEUM) and mandated the dissolution of several autonomous bodies, including the National Institute for Transparency, Access to Information, and Protection of Personal Data (INAI), the Federal Economic Competition Commission (COFEC), and the Federal Telecommunications Institute (IFT)¹²⁸.

The Mexican government has advocated for the streamlining and centralization of government agencies as a measure aimed at improving administrative efficiency. According to its proposals, this

¹²⁷Mexico. (February 5, 1917). Political Constitution of the United Mexican States. Official Gazette of the Federation. <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>

¹²⁸Chamber of Deputies. (2024, December 20). *DOF publishes decree on constitutional reform regarding organizational simplification* (Note No. 1268). Public Relations: News Agency. <https://comunicacionsocial.diputados.gob.mx/index.php/notilegis/dof-publica-decreto-de-reforma-constitucional-en-materia-de-simplificacion-organica>

restructuring will allow for more agile resource management, reduce operating costs, and promote greater coordination among various public policies.

At the same time, it is argued that existing models for competitiveness, telecommunications, and personal data regulation required modernization to adapt to the challenges of an increasingly globalized digital and economic context. The goal is for regulations to respond more effectively to the dynamics of digital platforms and cross-border information flows.

As part of this reform, it is proposed that so-called “regulated entities” in the areas of access to information and personal data protection be governed by a single, unified general law.¹²⁹ In the field of economic competition, the reform proposed a “new authority” to enforce policies and sanctions, lowering thresholds for merger reviews and strengthening the enforcement of services.¹³⁰ This measure seeks to standardize procedures and obligations, facilitating consistent and harmonized management throughout the country.

The reforms promoted by the Mexican government are highly significant at various levels. First, from a governance perspective, there is a profound redefinition of key regulatory and supervisory agencies, consolidating a more centralized structure and altering the role of traditional autonomous entities.

In the economic sphere, strengthening competition and regulating strategic sectors—particularly telecommunications—aims to foster investment and innovation. Furthermore, the goal is to reduce barriers to entry, thereby facilitating market access for new players and promoting greater dynamism in sectors historically dominated by a few companies.

Furthermore, regarding digital rights and data management, reforms in the areas of transparency and data protection seek to establish a new legal framework suited to the contemporary digital environment. For example, the proposed changes in the telecommunications sector require the Executive Branch, through the competent agency, to guarantee the right of access to information and communication technologies, as well as to broadcasting and telecommunications services, including access to broadband and the Internet.

The institutional impact of these reforms is evident in the dissolution of autonomous agencies and the transfer of their powers to the executive branch or to new entities. This process has sparked a broad debate on the need to maintain checks and balances, ensure transparency, promote accountability, and preserve regulatory autonomy. A clear example of this concern is the warning from various sectors about the potential weakening of mechanisms for accessing public information following the dissolution of the INAI.¹³¹

At the same time, the strengthening of competition law through the implementation of stricter sanctions and the lowering of thresholds for intervention seeks to send a clear signal of increased oversight and regulation to economic actors,¹³² which is particularly relevant in sectors characterized by the existence of barriers and concentration among a few dominant firms.

The legislative and constitutional reforms promoted in Mexico during the 2024–2025 period are primarily aimed at providing the Mexican government with up-to-date legal, institutional, and regulatory tools. The proponents of these reforms believe it is essential for the country to have modern

¹²⁹Mexico. (December 20, 2024). *Decree amending, adding, and repealing various provisions of the Political Constitution of the United Mexican States regarding organizational simplification*. Official Gazette of the Federation. https://www.diputados.gob.mx/LeyesBiblio/legis/reflxvi/022_CPEUM_20dic24.doc

¹³⁰Guerrero Rodríguez, O. (2025, July 2). *Reforms to the Federal Economic Competition Law and the Abolition of COFECE and IFT*. Hogan Lovells. <https://www.hoganlovells.com/es/publications/reforms-to-the-mexican-competition-law-cofece-and-ift-extinction>

¹³¹Piña, G. (2025, July 11). *Mexico’s Lack of Transparency: Opacity and Media Restrictions*. Diálogo Político. <https://dialogopolitico.org/agenda/opinion-agenda/democracia-opaca-mexico-transparencia>

¹³²Guerrero Rodríguez, O. (July 2, 2025). *Reforms to the Federal Economic Competition Law and the Abolition of COFECE and IFT*. Hogan Lovells. <https://www.hoganlovells.com/es/publications/reforms-to-the-mexican-competition-law-cofece-and-ift-extinction>

mechanisms to address contemporary challenges, including the digital economy, the presence of highly concentrated markets, the need for universal connectivity, and the proper management of personal data.

In this context, the goal is to improve the efficiency of the state apparatus by reducing bureaucracy and simplifying structures. This evolution aims to align Mexican regulatory institutions with the demands and dynamics of a globalized environment, characterized by rapid technological evolution and the growing interdependence of markets.

Essentially, the goal of the reforms is to redefine the regulatory framework in key areas such as transparency, personal data protection, economic competition, and telecommunications. Their purpose is to expand citizens' access to digital services, ensure greater competition in the markets, and promote a more agile and less fragmented public administration. All of this responds to the need to adapt the State and its institutions to the demands of the 21st century, facilitating Mexico's integration into the global digital economy and ensuring the protection of citizens' rights in the digital environment.

7.2 Freedom of Expression and Human Rights

Mexico formally recognizes freedom of expression and of the press in Articles 6 and 7 of its Constitution, which guarantee the free dissemination of opinions and ideas. This legal framework is complemented by the incorporation into the constitutional order of the Universal Declaration of Human Rights and the American Convention on Human Rights, which impose on the State the inalienable obligation to protect the active exercise of the right to seek, receive, and disseminate information. Despite this formal regulatory and democratic framework, freedom of expression in the country faces systemic challenges, characterized by a highly dangerous environment for the practice of journalism.

Physical and institutional violence poses the greatest challenge to freedom of expression and freedom of the press. Mexico is consistently ranked as one of the most dangerous countries in the world for journalists, a fact reflected in its drop of three positions in RSF's 2025 World Press Freedom Index¹³³. This situation is exacerbated by the infiltration of organized crime into public life, which gives rise to hybrid forms of interference in which criminals—often in collusion with local authorities—coerce the press. This dynamic has led to the emergence of “silenced zones” throughout the country, where self-censorship prevails, limiting journalists in what they can publish or forcing them to disseminate messages dictated by organized crime. All of this operates under the cloak of structural impunity, where 99.6% of crimes against the press go unpunished.

The right to freedom of expression is defined as the right that allows people to seek, receive, and disseminate information and ideas of any kind, thus constituting one of the essential pillars of democratic societies. This right takes on particular significance during elections, when free access to information about candidates, proposals, and party platforms is indispensable for citizens to form their opinions and make informed decisions.

In this regard, during election periods, states bear the responsibility of ensuring conditions conducive to the full exercise of freedom of expression. It is essential to foster a free and open environment in which the debate of ideas can take place without undue restrictions. To achieve this, the government must refrain from implementing any form of censorship, whether direct or indirect, ensuring that information of public interest is available to citizens.

¹³³ Reporters Without Borders. (2025, May 3). *2025 World Press Freedom Index*. <https://rsf.org/es/clasificacion-mundial-de-la-libertad-de-prensa-rsf-2025>

Although the State has implemented formal mechanisms such as the Law for the Protection of Human Rights Defenders and Journalists (2012)¹³⁴ and its corresponding Protection Mechanism at the federal level, these bodies operate with severe budget shortfalls, a lack of trained personnel, and coordination issues with local authorities. Additionally, the Special Prosecutor's Office for Crimes Against Freedom of Expression (FEADLE) has failed to dismantle impunity or restore public trust; it frequently dismisses the link between the crimes and the victims' journalistic work, and has suffered severe budget cuts that undermine its investigative capabilities.

Security challenges also present acute intersectional vulnerabilities that exacerbate the risk for certain groups. Community and Indigenous journalists face constant physical attacks and racial discrimination, often operating in remote areas with limited resources and under siege by non-state actors. For their part, women journalists must contend with specific forms of harassment, online violence, workplace inequality, and a glaring lack of a gender perspective in criminal investigations and state protection measures.

Beyond physical violence, freedom of expression is under attack through tactics of criminalization, indirect censorship, and political hostility. In 2025, judicial harassment against journalists increased by 143%, with prosecutors' offices and courts being used to pressure reporters through defamation lawsuits. There is a misuse of civil lawsuits filed by public officials demanding exorbitant financial compensation, creating a deliberate deterrent effect on journalistic investigations. Added to this pressure is the constant stigmatization of activists and critical media outlets at government press conferences—a practice that has gone so far as to publicly disclose the personal information of international journalists.

Furthermore, in 2024, Congress approved reforms to abolish key independent agencies such as the National Institute for Transparency, Access to Information, and Protection of Personal Data (INAI)¹³⁵, which fosters a culture of opacity that makes it easier to conceal information about human rights violations.

Finally, the media and digital ecosystem faces regulatory obstacles that restrict pluralism. The discretionary allocation of government advertising persists as a long-standing mechanism of editorial control, lacking objective standards to prevent abuse and the excessive spending of public resources.

In the digital sphere, the outlook is clouded by the prevalence of unsupervised surveillance and espionage against human rights defenders and journalists. Furthermore, recent telecommunications reforms empower authorities to remove content from platforms based on government criteria that may be ambiguous. Taken together, this multitude of physical, institutional, legal, and digital challenges severely compromises the right of Mexican citizens to be informed in a free, pluralistic, and secure manner.

Online freedom of expression in Mexico has faced a significant deterioration, marked by an increase in violence and the use of legal mechanisms for censorship, which poses a challenge to the public sphere and democracy. The situation is characterized by persistent physical and psychological attacks against journalists and communicators, as well as the implementation of new intimidation strategies. Violence does not come solely from non-state actors; the authorities themselves remain the primary perpetrators, as reported in the 2024 report by the civil society organization *Freedom House*,¹³⁶ and highlighted by the Network in Defense of Digital Rights (R3D).

¹³⁴Mexico. (June 25, 2012). *Law for the Protection of Human Rights Defenders and Journalists*. Official Gazette of the Federation. https://www.gob.mx/cms/uploads/attachment/file/460775/Ley_para_la_Proteccion_de_Personas_Defensoras_de_Derechos_Humanos_y_Periodistas.pdf

¹³⁵Mexico. (December 20, 2024). Decree amending, adding, and repealing various provisions of the Political Constitution of the United Mexican States regarding organizational streamlining. Official Gazette of the Federation. https://www.dof.gob.mx/nota_detalle.php?codigo=5745814&fecha=20/12/2024#gsc.tab=0

¹³⁶Freedom House, "Freedom on the Net 2024," *Freedom on the Net, Key Developments*, Freedom House (U.S.), May 31, 2024, <https://freedomhouse.org/country/mexico/freedom-net/2024>.

For example, content moderation in Mexico has a direct impact on journalistic work, particularly due to internal decisions made by social media platforms and web hosting services through the “*notice and takedown*” mechanism. This procedure has led to the removal of news reports produced by journalists, activists, and other civil society actors, on the grounds of alleged copyright infringements by third parties. However, in most cases, the content was entirely the original work of the affected journalist, thereby limiting the exercise of freedom of expression both as a creator and as a citizen.

The notices supporting these removals cite the U.S. Digital Millennium Copyright Act (DMCA).¹³⁷ This law allows copyright holders to send a notice to the service provider requesting the immediate removal of allegedly infringing content, often without a legal review process but rather through automated systems.¹³⁸ The result is the removal of legitimate content, which hinders the flow of information and restricts the right to freedom of expression for journalists and citizens.

During the 2024 election cycle, the digital conversation in Mexico was characterized by the growing presence of disinformation and the use of generative artificial intelligence. These factors contributed significantly to social polarization and mistrust of both the media and various organizations. The proliferation of false information and the manipulation of content created informational confusion among citizens,¹³⁹ undermining society’s ability to discern truthful and reliable sources. As a result, there was a noticeable erosion of public trust in both traditional and digital news outlets.

In parallel with the issue of disinformation, the National Electoral Institute (INE) intervened by granting provisional measures in favor of female candidates who reported gender-based political violence allegedly perpetrated by journalists, columnists, and digital media outlets. This institutional action highlights the complexity of the digital environment, where efforts to protect fundamental rights can conflict with journalistic work and the exercise of freedom of expression.¹⁴⁰ The process underscored the need to strike a balance between protecting vulnerable groups and respecting the right to report and express opinions in the digital space.

By 2025, the national political debate centered on a proposed reform of the Telecommunications Law, which included the authority to block digital platforms. This provision was criticized by various observers as a potentially censorial measure, capable of restricting freedom of expression and access to information. In light of the controversy, President Claudia Sheinbaum¹⁴¹ chose to halt the reform process and convened thematic roundtables with experts to discuss and review the controversial article. This episode illustrated the tensions between the need to regulate the digital ecosystem and the importance of safeguarding fundamental rights online—an ongoing struggle in which civil society organizations, academics, and digital regulation specialists actively participated.

Digital surveillance and the use of spyware, such as Pegasus, continue to be a source of political and social concern. In 2025, the Special Rapporteur for Freedom of Expression of the Inter-American

¹³⁷Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (1998). <https://www.copyright.gov/legislation/dmca.pdf>

¹³⁸McSherry, C. (September 16, 2020). *Notice and takedown mechanisms: Risks for freedom of expression online* [Written statement]. Electronic Frontier Foundation. https://www.eff.org/files/2020/09/04/mcsherry_statement_re_copyright_9.7.2020-final.pdf

¹³⁹Reuters Fact Check. (May 27, 2024). *Fact Check: French university did not conduct studies predicting the outcome of the Mexican elections*. Reuters. <https://www.reuters.com/world/americas/verificacion-universidad-francesa-no-realizo-estudios-con-pronostico-sobre-elecciones-en-2024-05-27/>

¹⁴⁰Special Rapporteur on Freedom of Expression. (2017). *Standards for a Free, Open, and Inclusive Internet*. Inter-American Commission on Human Rights. https://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf

¹⁴¹Raziel, Z. (April 25, 2025). Sheinbaum Puts the Telecommunications Law on Hold Following Controversy Over the Provision Allowing the Government to Block Digital Platforms. El País. <https://elpais.com/mexico/2025-04-25/sheinbaum-frena-la-ley-de-telecomunicaciones-tras-la-polemica-por-el-articulo-que-permitia-al-gobierno-bloquear-las-plataformas-digitales.html>

Commission on Human Rights (RELE CIDH,¹⁴²) compiled evidence of espionage cases in Mexico, including significant incidents that occurred in 2023. These practices affected journalists, academics, and individuals involved in sensitive investigations, adding to campaigns of harassment and *doxxing* aimed at intimidating and driving critical voices out of the public sphere. Taken together, disinformation, ambiguous regulatory proposals, intimidating litigation, and surveillance constitute the main current challenges to online freedom of expression in Mexico.

7.3 Digital Environment

In recent years, Mexico has experienced sustained growth in its digital infrastructure, allowing connectivity to reach increasingly broad sectors of the population, including children and adolescents. According to the 2024 National Survey on the Availability and Use of Information Technologies in Households (ENDUTIH), published by INEGI in May 2025¹⁴³, an estimated 100.2 million people aged six and older use the internet, representing 83.1% of the Mexican population in that age group. This represents an increase of nearly two percentage points compared to the previous year, cementing internet access as a fundamental part of daily life for interaction, education, and entertainment.

The ENDUTIH study provides a comprehensive overview of access to and use of digital devices in Mexican society. It highlights the role of groups with higher internet penetration rates. In particular, for example, 95.1% of adolescents aged 12 to 17 are active users, a figure very close to the 97% of young adults aged 18 to 24. Meanwhile, the 6- to 11-year-old age group also maintains high levels of access, although the average daily time spent online is lower than that of adolescents and young adults. In 2024, children aged 6 to 11 reported an average of 2.6 hours of daily internet use, while adolescents aged 12 to 17 averaged 3.0 hours per day. These data reflect that Mexican children are entering the digital environment at an early age and with varying levels of intensity.

The 2024 ENDUTIH survey indicates that 97.2% of internet users in Mexico connect via a smartphone, confirming mobile phones as the primary tool for digital access. This pattern is particularly relevant for minors, as it facilitates mobility and immediate access to social media, educational platforms, and entertainment content. In addition, 43.6% of users use smart TVs, 35.9% use computers (laptops, PCs, or tablets), and 8.1% access the internet via video game consoles. An illustration of this is provided in the table below, which shows the age range and the percentage of internet users, giving an approximation of the average daily device usage during the 2024 survey period.

Table 6. Internet Users in Mexico by Age Group

Age Group	% of Internet Users	Average Daily Hours of Use (2024)
6 to 11 years old	79.7%	2.6 hours
Ages 12–17	95.1%	4.5 hours
Ages 18–24	97.0%	5.7 hours
Ages 25–34	95.1%	5.6 hours
Ages 35–44	92.3%	4.7 hours

¹⁴²Special Rapporteur on Freedom of Expression. (2025). *The Impact of Digital Surveillance on Freedom of Expression in the Americas* (OEA/Ser.L/V/II/CIDH/RELE/INF.33/25). Inter-American Commission on Human Rights. <https://www.oas.org/en/iachr/expression/reports/VigilanciaRELECIDH.pdf>

¹⁴³National Institute of Statistics, Geography, and Informatics. (2024). *National Survey on the Availability and Use of Information Technologies in Households (ENDUTIH) 2024*. <https://www.inegi.org.mx/programas/endutih/2024/>

Age Group	% of Internet Users	Average Daily Hours of Use (2024)
Ages 45–54	83.8%	3.9 hours
55 to 64 years old	71.0%	3.2 hours
65 years or older	42.1%	3.0 hours

Source: Author's own calculations based on ENDUTIH data.

It should be noted that significant differences in internet access still persist between urban and rural areas. According to ENDUTIH data, internet access in urban areas stands at 86.9%, while in rural areas it reaches only 68.5%. This highlights an urban-rural digital divide of nearly 18 percentage points¹⁴⁴. Despite the progress made, structural barriers continue to affect children's and adolescents' access to digital resources, directly impacting their educational and developmental opportunities.

However, Mexico has been among the leading countries in terms of content removals on digital platforms, as demonstrated by a study published in 2020 titled *#LibertadNoDisponible*¹⁴⁵, which also establishes that content moderation on digital platforms affects freedom of expression and access to information. The main problems identified are:

- **Automated moderation:** Lack of contextual interpretation, which can result in undue censorship
- **Business models and platform architecture:** Designed for profitability, they can lead to exclusion and misinformation
- **Digital divide:** Limitations in infrastructure and connectivity affect equitable access to information

7.4 Digital Platforms Available in the Country

In Mexico, international digital platforms are not required to maintain a physical legal or corporate address in the country in order to operate and offer their services. However, following the tax reforms that took effect in 2020, the Tax Administration Service (SAT) requires foreign-based companies without a permanent establishment that provide digital services to users in Mexico to register with the Federal Taxpayers Registry (RFC). The purpose of this measure is to collect and withhold Value-Added Tax (VAT) and, in cases of intermediation (accommodation, transportation, delivery of goods), to withhold Income Tax (ISR) from creators and partners. According to the *List of Digital Service Providers Registered with the RFC*, published and updated bimonthly by the SAT, as of early 2026, there are dozens of global platforms (such as Meta, Amazon, Apple, Netflix, among others) formally registered to comply with these tax obligations (SAT, 2026).

These platforms' influence in the domestic market is extremely strong due to the country's high internet penetration rate. According to the *Digital 2024* report prepared by Kepios in collaboration with *We Are Social*, Mexico has more than 107 million internet users, of whom more than 90 million have active social media profiles. The estimated distribution of users (based on advertising reach reported by the platforms' own tools) is as follows:

¹⁴⁴Riquelme, R. (May 6, 2025). *100 million people now use the internet in Mexico: INEGI*. El Economista. <https://www.eleconomista.com.mx/tecnologia/100-millones-mexicanos-internet-mexico-inegi-20250506-757863.html>

¹⁴⁵Álvarez Pinzón, G. P., & Herrera Ortiz, M. (2025). *Freedom Not Available: The Setback of Digital Rights in the Face of Administrative Centralization in Mexico*. Journal of Law and Information Technology, 14(2), 45–68. <https://doi.org/10.1017/rdti.2025.102>

Table 7. Distribution of Users by Digital Platform in Mexico

Platform	Number of users (in millions)
Facebook	90.20
TikTok	74.15
Instagram	44.85

Source: Compiled by the author based on the "Digital 2024: Mexico" report by We Are Social and Kepios. (Note: The TikTok figure includes only users aged 18 and older.)¹⁴⁶

In the area of political and electoral affairs, the National Electoral Institute (INE) regularly enters into agreements and memoranda of understanding with major technology companies (including Meta, TikTok, Google, and X), with a special focus on particularly sensitive periods such as the 2024 federal elections. As in the Costa Rican experience, signing these agreements opens direct channels for institutional cooperation, although these depend on the agreements remaining in effect.

These efforts focus on protecting electoral integrity, combating misinformation (through partnerships with fact-checkers and tools such as the official WhatsApp chatbot), and establishing fast-track channels for reporting illegal content.

In terms of oversight, political parties have a legal obligation to report their digital campaign expenditures to the INE; however, establishing a unified and comprehensive tracking system for all advertising spending invested directly on platforms continues to pose a technical and regulatory challenge for the agency.

7.5 Legislative and Regulatory Context in Mexico

7.5.1 Constitutional Framework

The Mexican constitutional framework grounds the protection of rights in the digital environment primarily in Articles 6 and 7 of the Constitution, which guarantee freedom of expression, the freedom to disseminate opinions on any subject, and the express prohibition of prior censorship. These guarantees fully extend to the use of the internet, social media, and other information and communication technology (ICT) platforms, establishing that the expression of ideas shall not be subject to judicial or administrative scrutiny, with the sole limitations pertaining to attacks on public morals, the violation of third-party rights, the incitement of a crime, or the disruption of public order. In keeping with this spirit of safeguarding rights, the Supreme Court of Justice of the Nation has reinforced digital privacy by ruling that personal communications are protected against state interference in the absence of a prior court order, except in very strict cases related to national security.

The right to freedom of expression is a right that allows individuals to seek, receive, and disseminate information and ideas of any nature, thus constituting one of the essential pillars of democratic societies. This right takes on particular significance in electoral contexts, where free access to information about candidates, proposals, and party platforms is indispensable for citizens to form their opinions and make informed decisions.

Despite these solid foundations, the legal system faces profound tensions as it attempts to adapt its regulations to the contemporary challenges of the digital ecosystem. On the one hand, recent

¹⁴⁶Kemp, S. (2024, February 21). *Digital 2024: Mexico*. We Are Social; Kepios. <https://datareportal.com/reports/digital-2024-mexico>

proposals to reform the Telecommunications Law have raised international concerns due to the possible inclusion of controls that would empower the government to block digital platforms without a court order. On the other hand, there is a public and legislative debate regarding the need to establish regulations to address phenomena such as cyberbullying, digital gender-based violence, misinformation, and hate speech. All of this frames Mexico's current challenge: to find a regulatory and operational balance that fully preserves citizens' right to seek, receive, and disseminate information, without neglecting social responsibility and risk mitigation on these platforms.

An analysis of Mexican legal provisions reveals a significant effort to adapt the traditional legal framework to the current reality of platforms and the digital environment. There is a clear trend toward creating specific obligations for Online Service Providers (OSPs) and other digital actors, with the aim of regulating their conduct regarding the protection of personal data.

7.5.2 Telecommunications and Media Legislation

The Law on Telecommunications and Broadcasting (LMTR)¹⁴⁷ constitutes the regulatory framework governing the use and exploitation of the radio spectrum, telecommunications networks, and the provision of broadcasting services in Mexico. In today's digital landscape, the LMTR is of fundamental importance, as it establishes the basic rules for connectivity and network access—essential pillars for the operation of any digital platform in the country.

One of the central elements of the LMTR is the principle of Net Neutrality. This principle imposes on telecommunications concessionaires—that is, providers of internet services—the obligation to operate their networks impartially. In practical terms, this means they cannot unjustifiably discriminate against, block, or interfere with access to content, applications, services, or protocols. Net neutrality ensures that all users have free and equitable access to digital services, preventing providers from favoring or disadvantaging certain competitors in the digital environment.

In turn, the LMTR devotes specific sections to the protection of users' rights. Among the most relevant safeguards are service quality, transparent pricing, the ability to port telephone numbers, and the privacy of communications. These protections ensure that consumers can enjoy efficient and secure services, as well as switch providers without losing their number and with the assurance that their personal data will be safeguarded.

Furthermore, the LMTR imposes obligations on licensees to cooperate with competent authorities, such as the Attorney General's Office (FGR) and the Federal Judiciary (PJF). Two of the most relevant mechanisms in this regard are real-time geolocation and data retention. Concessionaires must provide geolocation data from mobile communication devices upon a specific court order, thereby facilitating criminal investigations. They are also required to retain traffic and connection data—known as metadata—which may be requested by authorities for the purposes of law enforcement.

The authority responsible for enforcing the LMTR is the Telecommunications Regulatory Commission (CRT), which has replaced the previous model of the Federal Telecommunications Institute (IFT). The CRT is a decentralized body attached to the Agency for Digital Transformation and Telecommunications (ATDT), which reports to the Federal Executive Branch. This institutional restructuring means that the CRT assumes key functions such as the regulation, promotion, and oversight of the radio spectrum; the protection of user rights; and the implementation of asymmetric measures to encourage competition among dominant economic actors.

Under the CRT's oversight, the principle of net neutrality remains an essential safeguard for Mexico's digital ecosystem. Internet service providers are prohibited from blocking, interfering with, discriminating against, or degrading internet traffic based on the content, application, origin, or

¹⁴⁷Mexico. (2025, July 16). *Federal Law on Telecommunications and Broadcasting*. Official Gazette of the Federation. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf>

destination of the data. This legal provision ensures that digital platforms and services, regardless of their size, provide equitable conditions for network access to all users.

The LMTR also retains the obligations of concessionaires to cooperate with security and law enforcement authorities, facilitating access to traffic data, metadata retention, and real-time geolocation exclusively under a court order. In summary, the regulatory essence of the LMTR regarding infrastructure and access remains in force, although oversight and enforcement are now concentrated in the CRT, operating under a renewed institutional governance model.

7.5.3 Specific Regulation of Platforms and/or Content Regulation

The Federal Economic Competition Law (LFCE)¹⁴⁸ has as its primary objective the regulation of the activities of relevant economic agents within the digital ecosystem. This includes, in particular, oversight of access to essential inputs, with the aim of ensuring free competition in markets that are increasingly dominated by digital platforms.

The LFCE grants powers to both the Agency for Digital Transformation and Innovation and the Market Regulatory Authority (ARM) to investigate and determine whether an economic agent holds substantial market power in a relevant market. This assessment is based on specific criteria, such as the existence of barriers to entry, the entity's ability to set prices without facing significant countervailing forces from competitors or consumers, and access to privileged information, including the handling of *big data*.

A central aspect within the digital environment is the essential input. In the context of platforms, this concept can encompass various elements indispensable for effective competition, such as critical network infrastructure, unique data and algorithms necessary to compete, or access to the user base of a dominant platform.

In cases where an economic agent with substantial market power exercises control over an essential input, the LFCE provides for the possibility of imposing specific measures aimed at ensuring that access to that input is granted on a non-discriminatory basis to competitors. This mechanism is key to preventing platforms with a dominant role from stifling competition through exclusive control of fundamental resources.

The law also prohibits so-called related monopolistic practices. Although these behaviors are not illegal in and of themselves, they become illegal when carried out by entities with substantial market power and have the effect of driving out competitors. Some examples of these practices, which are particularly relevant in the digital sector, include:

Tying: making the purchase of one product or service contingent on the purchase of another.

Denial of service: unjustifiably preventing access to a network or an essential input.

Cross-subsidization: using revenue obtained in a market where one holds dominance to finance predatory practices in another market.

In summary, the LFCE serves as the legal tool designed to regulate the market power of large platforms, ensuring conditions of effective competition and preventing such dominance from harming innovation and consumer interests.

The rise of e-commerce and the proliferation of online content have significantly transformed the landscape of consumer protection and copyright law. In light of this new scenario, the Federal

¹⁴⁸Mexico. (July 16, 2025). *Federal Economic Competition Law*. Official Gazette of the Federation. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFCE.pdf>

Consumer Protection Law (LFPC)¹⁴⁹ has adapted its provisions to ensure that providers comply with specific requirements related to e-commerce, transaction verification, and standard-form contracts. The core of this protection lies in ensuring the transparency of the information provided to consumers.

The LFPC, in Articles 76 Bis and 76 Bis 1, has been updated to provide specific protections for consumers who conduct transactions or contract for services through digital platforms. This approach is essential to ensuring that users' rights remain intact in the digital environment.

These protections are:

Clear and Accurate Information: Providers are required to provide complete and accessible information about goods, products, or services prior to purchase, including the total price, shipping costs, taxes, and warranty terms.

Complaint and verification mechanisms: Consumers must be able to file complaints or request clarifications through effective mechanisms, as well as verify their identity and the transaction to prevent fraud.

Standard-form contracts: The law regulates the use of online standard-form contracts, requiring them to be understandable and free of unfair terms. Additionally, providers must register these contracts and, in certain cases, obtain approval from the relevant authority.

The LFPC, together with the Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP), requires providers to ensure the security and confidentiality of consumers' personal and banking data. This involves the use of appropriate security protocols for card transactions, as well as a prohibition on using personal information for purposes other than those set forth in the privacy notice.

The Federal Consumer Protection Agency (PROFECO) acts as the authority responsible for enforcing and monitoring compliance with the LFPC, including in the digital sphere. PROFECO may implement remote conciliation procedures to resolve disputes between consumers and suppliers and has the authority to impose sanctions on suppliers that fail to comply with e-commerce requirements, such as a lack of transparency or failure to honor guarantees.

The LFPC seeks to ensure that consumers' rights are equal in both the physical and digital worlds. This results in an environment where transparency, security, and the ability to file complaints prevail, thereby protecting users of digital platforms.

The Federal Copyright Law (LFDA¹⁵⁰) directly addresses the issue of copyright infringement in the digital environment, establishing clear mechanisms to combat piracy and protect creators' rights. One of the central provisions is the *"notice and takedown"* obligation. Under this framework, platforms assume a fundamental responsibility: they must act diligently and in a timely manner to remove or disable access to material identified as infringing once they have received a formal notice from the rights holder or their representative, such as INDAUTOR.

The amendment to the LFDA incorporates a key distinction regarding the liability of Online Service Providers (OSPs), who act as intermediaries by hosting or transmitting content. Under the law, OSPs will not be liable for infringements committed by their users, provided they fulfill their duty to act promptly upon receiving notices of infringing content. This mechanism limits their general liability and establishes their role as agents that contribute to the enforcement of copyright, without turning them into censors or subjecting them to unlimited liability.

The system operates through two main mechanisms. First, the notice-and-takedown procedure, whereby the rights holder notifies the OSP of the infringement, and the OSP must remove or block

¹⁴⁹Mexico. (December 26, 2024). Federal Consumer Protection Law. Official Gazette of the Federation. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPC.pdf>

¹⁵⁰Mexico. (July 1, 2020). Federal Copyright Law. Official Gazette of the Federation. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFDA.pdf>

access to the material in question. Second, the counter-notice mechanism, which gives the affected user the opportunity to respond and argue that their content does not infringe copyright or that the removal was erroneous. In this case, the PSL must inform the rights holder of the counter-notice received.

This balance seeks to effectively protect copyright while also safeguarding users' rights, allowing for the legitimate use of material in certain cases—for example, under exceptions or limitations recognized by law. The procedure is, in essence, extrajudicial; however, it allows for the intervention of authorities such as INDAUTOR or the courts in the event of a dispute.

The National Copyright Institute (INDAUTOR) is established as the administrative authority responsible for mediating and resolving disputes arising from these notice, takedown, and counter-notice procedures. In this way, a specialized and efficient avenue is provided for the resolution of copyright-related conflicts in the digital environment, before resorting to judicial proceedings.

The introduction of Chapter IX Bis into the Federal Labor Law (LFT)¹⁵¹, which includes relevant articles such as 291-O and 291-P, constitutes one of the most significant actions taken by the Mexican government in the realm of the digital economy. The fundamental purpose of this reform is to formalize the employment relationship between digital platforms and the workers who provide services on them, putting an end to the debate over their status as independent contractors.

The findings of the research highlight that the spirit of the law is to ensure clear channels of transparency and protection for this labor sector, particularly in light of the algorithmic control mechanisms that are an essential part of digital platforms' operations. The regulation places special emphasis on algorithmic governance by requiring platforms to digitize and make transparent their rating standards and to implement appeal mechanisms against arbitrary deactivations.

This means that any automated decision affecting workers' continued employment or income must be duly justified and subject to review. In this way, workers are protected from a work environment where decision-making is mediated by algorithms, allowing for oversight and recourse against potential arbitrary actions.

The reform also provides for the recognition of specific labor rights, such as the right to participate in profit-sharing (PTU) provided that a minimum annual work hours requirement is met, the obligation to pay for services on a weekly basis, and the application of existing regulations regarding occupational safety and health.

In summary, the LFT adopts a hybrid regulatory model: on the one hand, it recognizes the flexibility inherent in work on digital platforms; on the other, it establishes traditional obligations that ensure a minimum level of social and legal protection. All of this is overseen by the Ministry of Labor and Social Welfare (STPS) and the labor courts, which ensure compliance with and the defense of these rights.

The inclusion of specific provisions in the Federal Criminal Code (CPF)¹⁵² to address crimes committed through electronic means represents a crucial step forward in tackling the challenges of cybercrime in Mexico. Articles 11 Bis, 424 Bis, and 461 Bis constitute the essential criminal law framework for prosecuting crimes in the digital environment, thus marking the transition from traditional crime to more sophisticated and technologically advanced forms. This legal recognition implies that technology can not only be used as a means to commit crimes but can also, at times, become the very object of the crime itself. Consequently, the CPF has been updated to define and penalize specific conduct within cyberspace.

¹⁵¹Mexico. (February 21, 2025). Federal Labor Law. Official Gazette of the Federation. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFT.pdf>

¹⁵²Mexico. (November 28, 2025). Federal Criminal Code. Official Gazette of the Federation. <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf>

The Federal Criminal Code establishes penalties for those who unlawfully access, interfere with, or destroy computer systems and equipment, covering practices such as hacking, cracking, and the distribution of malware. The purpose of these provisions is to safeguard the integrity, confidentiality, and availability of both data and computer systems, thereby protecting the interests of individuals, businesses, and the State against digital threats.

In addition, the Federal Criminal Code penalizes the unauthorized dissemination of intimate images, cyberbullying, and child pornography. These offenses are prosecuted with strict coordination between the Federal Criminal Code (CPF), the Law on the Prevention and Punishment of Crimes Against Minors and Vulnerable Groups (LGAMVLV), and other laws aimed at protecting minors and vulnerable groups.

Article 11 Bis of the CPF places particular emphasis on the criminal liability of legal entities, that is, companies and digital platforms. If a digital crime is committed in the name of or on behalf of a legal entity, and this results from a lack of supervision or deficiencies in internal controls, the company may be penalized regardless of the liability of the individuals involved. Penalties range from fines and the closure of facilities to the permanent dissolution of the company, thereby establishing a legal framework that encourages the adoption of control and prevention measures within organizations.

The prosecution and punishment of digital crimes fall primarily under the jurisdiction of the Federal Judicial Branch (PJF) and the Attorney General's Office (FGR). These bodies have the authority to request court orders for digital searches, the seizure of equipment, and access to geolocation data or the preservation of metadata, in coordination with the LMTR. This evidence is essential in trials for crimes committed through electronic means, strengthening the State's investigative and prosecutorial capacity.

In summary, the CPF fulfills the essential function of establishing the punitive framework for unlawful conduct committed in cyberspace, for both individuals and companies, complementing existing administrative and civil laws. This comprehensive approach reinforces the protection of users' rights and legal certainty in Mexico's digital environment.

7.5.4 Data Protection and Privacy Legislation

The Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP)¹⁵³ constitutes the regulatory foundation for the responsible management of information by obligated entities, which include companies and digital platforms. This law focuses on ARCO rights, privacy notices, and the regulation of data transfers, promoting transparency and accountability.

The LFPDPPP establishes a series of guiding principles for the processing of personal data:

- **Lawfulness:** Processing must be carried out in accordance with the law.
- **Consent:** The data subject's consent must be obtained.
- **Information:** The data subject must be informed about the use of their data.
- **Quality:** Data must be accurate, complete, and up-to-date.
- **Purpose:** Data must be used only for the specified purposes.
- **Fairness:** Data processing must be conducted in an honest and transparent manner.
- **Proportionality:** Only the data necessary to fulfill the purpose should be processed.
- **Accountability:** The data controller must ensure compliance with regulations and the protection of data.

¹⁵³ "Federal Law on the Protection of Personal Data Held by Private Parties," Official Gazette of the Federation, March 20, 2025, <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.

The privacy notice is the essential legal instrument that embodies the principle of information. It explains to the data subject how their data will be used and the mechanisms available to exercise their rights.

For their part, the ARCO Rights (Access, Rectification, Cancellation, and Opposition) allow data subjects to exercise control over their personal information. Digital platforms are required to facilitate the exercise of these rights, which are detailed below:

- Access: The right to know what data is held and for what purposes it is used.
- Rectification: The right to request the correction of incomplete or inaccurate data.
- Deletion: The right to request the deletion of data once the purpose of processing has been fulfilled.
- Objection: The right to object to the processing of data for specific purposes.

One of the key issues for digital platforms—especially those that operate globally or outsource services—is the regulation of data transfers. The LFPDPPP requires that, in order to transfer data to third parties—whether domestically or internationally—the data subject’s consent must be obtained, except in cases of exception provided for by law. Furthermore, the recipient of the data must assume the same protection obligations, ensuring that the level of protection is not diminished, regardless of the entity or country processing the data.

The powers of oversight, supervision, and enforcement regarding personal data protection have been transferred to the Secretariat for Anti-Corruption and Good Governance. Within this Secretariat operates the new Federal Data Protection Authority—also referred to in some sources as “Transparency for the People”—which is responsible for ensuring compliance with the regulations and imposing penalties for violations related to the processing of personal data.

The new law, published on March 20, 2025, repeals the 2010 law and consolidates several changes that directly impact businesses and digital platforms:

Key Aspect	Amended Provision / New Obligation
Definition of Data	The definition of “Personal Data” is slightly expanded, and the limitation that it applies only to natural persons is removed, now covering any identifiable person whose identity can be determined indirectly.
Consent	It is specified that consent must be freely given, specific, and informed. However, the law establishes that, as a general rule, implied consent will be valid, which simplifies certain <i>compliance</i> processes.
Transfers	There is a stricter requirement to obtain consent again when intending to process data for purposes other than those set forth in the original privacy notice. This limits the ability to use data for compatible or analogous purposes.
Confidentiality	The confidentiality obligation is clearer and more comprehensive. It requires the Data Controller (the platform) and third parties to implement specific controls or mechanisms to ensure the confidentiality of the data by all persons involved in the processing.

Cookie Regulations	Although it is not yet fully in effect, the law includes a ban on the use of deceptive or manipulative designs (<i>dark patterns</i>) to obtain consent for identification and tracking files on the web (<i>cookies</i> and digital profiling techniques), along with a specific penalty system.
Appeal Procedures	Decisions issued by the new Secretariat for Anti-Corruption and Good Governance may now be challenged directly through amparo proceedings before specialized courts and tribunals.

7.5.5 Specific Regulations for the Protection of Vulnerable Groups

The General Law on Women's Access to a Life Free of Violence (LGAMVLV)¹⁵⁴ has undergone significant evolution to recognize and address digital and media violence. This transformation responds to the need to protect women from new forms of aggression emerging in the virtual environment and establishes specific legal mechanisms to address these threats.

The LGAMVLV provides clear definitions of digital violence and media violence, expressly recognizing that acts such as harassment, defamation, and the non-consensual dissemination of intimate content are increasingly occurring in cyberspace. In this regard, the law empowers various authorities, including the Attorney General's Office (SEGOB) and local authorities, to intervene in a timely manner.

Among the most significant mechanisms are the ability to issue orders to remove content and the implementation of protective measures, which provide the legal authority to require digital platforms or service providers to remove, block, or take down digital material that constitutes a form of violence, such as in cases of revenge porn or the dissemination of intimate images without consent.

The regulation also highlights the importance of safe access to information and communication technologies (ICT) and the adequate safeguarding of databases as part of protection strategies. Agencies such as the National System for the Comprehensive Protection of Children and Adolescents (SIPINNA), the INM-COMAR, and state attorney general's offices are actively involved, demonstrating a comprehensive approach aimed at protecting particularly vulnerable groups—such as children, adolescents, and migrant women—who are at greater risk of online exploitation and violence.

This law establishes a robust institutional framework to guarantee women's safety in the digital and media spheres. This framework ensures an effective and prompt legal response to halt acts of aggression perpetrated through electronic means, thereby consolidating effective protection against gender-based violence in the digital environment.

Furthermore, the Federal Criminal Code criminalizes the unauthorized dissemination of intimate images, cyberbullying, and child pornography. These offenses are prosecuted through strict coordination between the Federal Criminal Code (CPF), the LGAMVLV, and other laws aimed at protecting minors and vulnerable groups.

The reforms known as the "Olimpia Law" have primarily amended the LGAMVLV, but the Federal Criminal Code also incorporates and complements these provisions, especially those related to the dissemination of sexually intimate content without consent. In addition, there are recent initiatives

¹⁵⁴Mexico. (December 16, 2024). *General Law on Women's Access to a Life Free of Violence*. Official Gazette of the Federation. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf>

aimed at reforming articles such as Article 199 Octies, with the goal of including the manipulation of images using Artificial Intelligence (AI) as a form of violation of sexual privacy.

7.5.6 Digital Electoral Regulation

Mexico's electoral regulatory framework is based on a constitutional design that entrusts the administration and oversight of elections to two autonomous bodies: the National Electoral Institute (INE) and the Federal Electoral Tribunal (TEPJF). The integrity of the electoral process is safeguarded by the Constitution and a set of general laws that guarantee citizens' political rights, including the equitable participation of indigenous communities and women. A recent example of the defense of institutional certainty and integrity was the 2023 ruling by the Supreme Court of Justice of the Nation, which invalidated a series of proposed reforms due to violations of legislative procedure, thereby ensuring the stability of democratic rules prior to elections and the independence of the authorities responsible for overseeing the process.

In close alignment with the standards of the Inter-American Human Rights System, Mexican law recognizes that freedom of expression and access to information (enshrined in Article 6 of the Constitution under the principle of maximum transparency) are fundamental pillars during electoral cycles. Censorship-free political debate is viewed as an essential tool for shaping informed public opinion and enabling citizen oversight. This approach requires that any restriction on communication rights be exceptional, reasonable, and strictly comply with the criteria of legality, necessity, and proportionality, safeguarding pluralism against any attempt to suppress dissenting voices.

In the face of growing digital threats, the electoral system has developed legal mechanisms to combat disinformation and online toxicity that could distort the will of the people. Article 41 of the Constitution expressly prohibits defamation in political propaganda. At the local level, legislation such as Mexico City's Electoral Code¹⁵⁵ goes a step further by expressly penalizing "negative campaigns" on social media and internet platforms. These regulations cover the dissemination of false information that undermines dignity, hate speech, and gender-based political violence. To mitigate these risks swiftly, the INE and the TEPJF have the authority to implement special sanctioning procedures and issue precautionary measures, such as the immediate suspension or removal of content, with the aim of protecting the fairness of the election.

In terms of technological integrity and data security, the National Cybersecurity Strategy¹⁵⁶ serves as an overarching framework. With the implementation of methods such as online electronic voting (SIVEI) for residents abroad, the government has deployed rigorous physical, administrative, and technical controls. The measures implemented include biometric voter authentication, cryptographic separation of identity and voting to guarantee the secrecy of the ballot, and the application of international security standards (ISO/IEC 27002:2013). All of this prevents cyberattacks and algorithmic tampering and safeguards citizens' privacy.

¹⁵⁵Mexico City Congress. (2024, June 7). *Code of Electoral Institutions and Procedures of Mexico City*. Official Gazette of Mexico City. <https://www.congresocdmx.gob.mx/media/documentos/014c22744927f99990f1190c1071da5184852083.pdf>

¹⁵⁶Mexico. Government of the Republic. (2017). *National Cybersecurity Strategy*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_de_Ciberseguridad.pdf

7.6 Alignment with UNESCO Guidelines: Mexico

An analysis of Mexico's alignment with the UNESCO Guidelines reveals a conceptual convergence regarding the protection of human rights, with a special emphasis on the safeguarding of personal data and the criminalization of new forms of technology-facilitated violence, as set forth in the General Law on Women's Access to a Life Free of Violence (LGAMVLV).

The regulatory framework is robust and far-reaching, firmly grounded in constitutional principles and international treaties that explicitly protect freedom of expression, privacy, and access to information in the digital environment. The legal framework covers a broad regulatory scope involving social media platforms, e-commerce, and infrastructure providers. There are specialized laws such as the Federal Economic Competition Law (LFCE), the Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP), and the recent amendments to the Federal Labor Law (LFT).

The aforementioned LGAMVLV criminalizes new forms of technology-facilitated violence against women and undoubtedly represents a step forward in their protection, serving as a model for the protection of other vulnerable groups. However, the effectiveness of these formal safeguards clashes head-on with the country's operational reality, where the full exercise of digital rights is severely hampered by challenges such as systematic violence against journalists and the documented use of state surveillance tools.

Mexican law already provides for a "high threshold" for restrictions on freedom of expression, exemplified by the three-part test of legality, necessity, and proportionality, as detailed in both legal dissertations and the case law of the Supreme Court of Justice of the Nation (SCJN). For its part, copyright law provides for a conditional liability regime for intermediaries similar to "safe harbor" provisions, exempting platforms from liability *a priori* for third-party content, provided they respond diligently to notices of infringement.

However, issues such as transparency and accountability on the part of authorities regarding their requests to restrict content on digital platforms—as established by UNESCO—still require explicit and robust legal provisions within the Mexican regulatory framework. This vulnerability is exacerbated by the lack of a cross-cutting legal mandate requiring platforms to be transparent about their moderation decisions or to undergo audits on the impact of their algorithms on individuals' rights. While sector-specific remedies do exist—such as in the aforementioned case of copyright, the right to challenge for digital platform workers, and ARCO rights in the context of data protection—clearer and more effective avenues are needed to appeal arbitrary moderation decisions based on private terms of use in other contexts.

The most profound divergence from the standards promoted by UNESCO lies in Mexico's institutional design and regulatory governance. Although the legal framework prohibits prior censorship and enshrines the principle of net neutrality, the structural reforms passed between 2024 and 2025 have reduced—or even eliminated—the constitutional autonomy of key regulators in the areas of telecommunications, economic competition, and transparency (such as the IFT, COFECE, or INAI), whose functions were absorbed by agencies of the Executive Branch. This concentration of powers directly contravenes the Guidelines' recommendation to have regulatory bodies that are strictly independent of political and economic control, thereby weakening institutional safeguards against arbitrary government intervention or disproportionate surveillance.

In the electoral sphere, there is significant alignment between the protective framework for human rights and freedom of expression enshrined in Mexican law and the UNESCO Guidelines. Mexico's electoral legislation and the rulings of its highest courts require a high threshold of safeguards to restrict public discourse, with the application of the three-part test of necessity and proportionality—established in international law and promoted by UNESCO—being *a sine qua non*. Furthermore, the

legal criminalization of digital gender-based violence and hate speech in electoral contexts reflects an alignment with the urgent need to protect vulnerable groups and mitigate risks to electoral integrity in the digital ecosystem. To this end, electoral authorities enjoy the independence required by international standards.

And although the Mexican government acts to curb abuses through precautionary measures and legal rulings, its response to technology platforms continues to operate primarily through collaboration agreements with the platforms and *ad hoc* reactions. It would be advisable to work toward a comprehensive legal framework that incorporates statutory obligations regarding due diligence, algorithmic transparency, and accountability—requiring platforms to proactively assess and mitigate how their moderation and recommendation systems amplify electoral disinformation, while ensuring that this does not lead to government controls that jeopardize free democratic debate.

Finally, the government's approach to systemic disinformation remains fragmented and insufficient; although authorities such as the INE have implemented provisional measures during electoral processes, there is still a need to develop a comprehensive regulatory strategy to address these phenomena without jeopardizing freedom of expression. At the same time, efforts to digitally empower citizens would be strengthened by more robust national policies on media and information literacy.

8. Country Analysis: Panama

8.1 Political and Legal System

The Republic of Panama is governed by the 1972 Political Constitution of the Republic of Panama (CPRP),¹⁵⁷ which is the fundamental law establishing it as a presidential republic with a democratic system of government based on the separation of powers among three branches: executive, legislative, and judicial. Its constitution consists of 328 articles, including a preamble and 15 titles. Its provisions establish the structure of the Panamanian State (Articles 1–7), the conditions for nationality and foreign residency (Articles 8–16), an extensive section on both individual and social rights and duties (Articles 17–130), and another section on political rights (Articles 131–145). The legislative (Art. 146–174), executive (175–200), and judicial (201–224) branches are described below.

Territorial organization is divided into municipal and provincial systems (Articles 225–256), public finance (257–281), guidelines governing the national economy (Articles 282–298), and provisions regarding public servants (299–309) and law enforcement (310–312). The process for amending the Constitution is set forth in Articles 313 and 314, and there is a title dedicated to the Panama Canal (Articles 315–323)—the most important of the country’s national infrastructure projects—as well as a section on final and transitional provisions.

In addition to the three branches of government, there are other entities that are particularly relevant to the regulation and protection of rights in the digital sphere. Specifically, the Office of the Ombudsman is responsible for safeguarding fundamental rights (Art. 129 CPRP), which suggests that, by monitoring the actions, acts, or omissions of public officials, it must also oversee how these officials behave in digital environments and how the decisions they make may affect citizens’ rights in these spaces.

The Electoral Tribunal, which is autonomous and independent, is responsible for interpreting and applying the Electoral Law (¹⁵⁸) and for ruling on disputes arising from its application. Article 143 of the Constitution grants the Tribunal the authority to punish offenses and crimes against the freedom and integrity of the vote, from which it can be inferred that it has the power to punish such offenses and crimes originating in the digital sphere. The same article grants the Tribunal the power to initiate legislation in matters within its jurisdiction, meaning it has the authority to introduce electoral legislation aimed at mitigating any impact that digital platforms may have on the electoral process and its normal conduct.

For its part, Article 144 establishes the General Electoral Prosecutor’s Office as an “independent investigative agency that assists the Electoral Tribunal” and whose functions include safeguarding the political rights of Panamanian citizens. This means it has the authority to prosecute acts occurring in the digital environment that may interfere with the electoral rights of those citizens, as the Office is also tasked with prosecuting electoral crimes and offenses.

¹⁵⁷Panama. (1972). *Political Constitution of the Republic of Panama*. Official Gazette No. 17,210. (Amended by Legislative Acts No. 1 of 1983, Nos. 1 and 2 of 1993, No. 1 of 1994, and Constitutional Act No. 1 of 2004). https://www.gacetaoficial.gob.pa/gacetitas/25176_2004.pdf

¹⁵⁸Panama. (October 28, 2022). *Consolidated Text of the Electoral Code of the Republic of Panama* (Decree 60 of 2022). Official Gazette No. 29,652-A. https://www.gacetaoficial.gob.pa/gacetitas/29652A_2022.pdf

8.2 Freedom of Expression and Human Rights

The CPRP establishes a framework for the protection of human rights, although it separates individual and social rights (Articles 17–130) from political rights (Articles 131–145). Article 37 guarantees the free expression of thought without prior censorship, although it sets limits on expressions that undermine “the reputation or honor of individuals or social security or public order.”

Article 89 defines the media as “instruments of information, education, recreation, and cultural and scientific dissemination,” implying a duty to disseminate accurate information. Furthermore, Article 89 itself establishes that, if the media disseminate advertising or propaganda, “these must not be contrary to the health, morals, education, cultural development of society, and the national conscience,” referring to secondary legislation that must regulate the operation of these media. This constitutional provision opens the door to interesting discussions about the role of online media and its duty to contribute to healthy digital information environments that protect the interests and values reflected in this article.

For its part, Article 29 declares the inviolability of private communications. Article 42 establishes the right to access and rectify personal data, and Article 43 guarantees access to public information. These are complemented by Article 41, which establishes the rights to petition and file complaints, and—most relevant to our study—Article 49, which enshrines the rights of consumers and users to quality services and accurate information about goods and services (which would affect how they are advertised online).

The International Covenant on Civil and Political Rights (ICCPR) and Law 79 of 2013 (Budapest Convention) are also ratified.¹⁵⁹ Furthermore, Article 5 of the Panamanian Penal Code¹⁶⁰ establishes that the human rights provisions of the Constitution and international conventions are an integral part of said code, thereby guaranteeing rights in the criminal sphere.

The judicial system is responsible for judicial protection of human rights, while the National Authority for Transparency and Access to Information (ANTAI) exercises administrative oversight regarding personal data. The aforementioned Ombudsman’s Office is responsible for the general protection of fundamental rights, while the Electoral Tribunal has exclusive jurisdiction over the protection of political communication rights and freedom of expression during campaigns.

Beyond constitutional, judicial, and administrative protections for human rights, various international organizations point to the diverse challenges facing freedom of expression, freedom of the press, and other rights in practice.

According to International IDEA’s , Panama scores highly in representation, and although it ranks among the top 25 countries in several categories, it remains in the middle range in terms of rights, the rule of law, and participation. The good news, according to IDEA, is that since 2019, indicators for freedom of expression and the reduction of economic inequalities have shown a positive trend. *Global State of Democracy Network*¹⁶¹

Freedom House considers Panamanian institutions to be democratic, with competitive elections and a rotation of power. With a Global Freedom Index score of 83 out of 100, Panama is considered a free country where freedom of expression and association are respected, although serious problems

¹⁵⁹United Nations. (December 16, 1966). *International Covenant on Civil and Political Rights*. Treaty Series, 999, 171. <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

¹⁶⁰Panama. (2022). *Penal Code of the Republic of Panama* (Consolidated Text published in the Official Gazette No. 29,514-A). Mizrahi & Pujol Publishing. https://www.organojudicial.gob.pa/uploads/wp_repo/assets/medias/leyes/codigo_penal_2022.pdf

¹⁶¹International IDEA. (2025). *Democracy Tracker: Panama*. <https://www.idea.int/democracytracker/country/panama>

of corruption and impunity persist, affecting both the highest echelons of government and the judicial system.¹⁶²

For its part, Reporters Without Borders (RSF) expresses concern over the frequent lawsuits filed against journalists who criticize government policies or expose corruption scandals, particularly those related to international financial scandals. According to its 2025 index assessment, which gives Panama a score of 66.75 and ranks it 53rd out of 180, there is evidence that media self-censorship is on the rise as the influence of government advertising in online media grows, limiting their independence¹⁶³.

The 2024 Country Report on Human Rights Practices, prepared by the U.S. Department of State, specifically notes that significant problems related to the protection of human rights persist in Panama, including restrictions on freedom of expression and media freedom. It concurs with RSF that harassment of journalists is a problem, and also noting that journalists engage in self-censorship to avoid reprisals from the government, political parties, and private-sector actors. The report also points out that threats against journalists are common from criminal groups when they investigate certain criminal activities. Nevertheless, according to the same report, the Panamanian government has taken credible steps to identify and punish public officials involved in human rights abuses.¹⁶⁴

The study on “Challenges to Freedom of Expression, the Rule of Law, and Democracy in Latin America” by the Baltasar Garzón International Foundation focuses on the case of SLAPPs (Strategic Lawsuits Against Public Participation) in Panama, a practice of judicial harassment against critical journalists and media outlets through defamation and libel suits and claims for moral damages. According to the report, judicial harassment is systematic, posing the main threat to press freedom alongside the severe difficulties in accessing public information in the country. This is largely, according to the report, because Panama’s laws provide limited protection for journalists, including the fact that defamation and slander are crimes that can lead to prison sentences—a situation exacerbated by the fact that Article 195 of the Panamanian Penal Code establishes that defamation and slander are considered aggravated offenses when committed by a media outlet. Although, on the other hand, there is an exemption from criminal penalties when the alleged victim of defamation or slander is a public official, this does not preclude civil liability arising from the acts, meaning that the risk of such lawsuits persists.¹⁶⁵

That said, a ruling by the Supreme Court of Justice of Panama represents a step in the right direction, as it sets an important precedent for the defense of freedom of expression and the protection of the right to information. The ruling reinforces the importance of the public interest in the right to information and analyzes in detail how the “actual malice” doctrine—established in the landmark U.S. Supreme Court case *New York Times v. Sullivan* (1964)—fits into Panamanian case law. It thus establishes parameters that better protect the work of journalists when reporting on public figures, stipulating that the plaintiff must demonstrate that the facts presented are indeed false. More importantly, the Supreme Court refers to the “chilling effect” of lawsuits against media outlets and journalists, noting that such actions constitute disproportionate remedies.¹⁶⁶

¹⁶²Freedom House. (2025). *Freedom in the World 2025: Panama*. <https://freedomhouse.org/country/panama>

¹⁶³Reporters Without Borders. (2025, May 2). *2025 World Press Freedom Index*. <https://rsf.org/es/clasificacion>

¹⁶⁴U.S. Department of State. (2025). *2024 Country Reports on Human Rights Practices: Panama*. Bureau of Democracy, Human Rights, and Labor. <https://www.state.gov/reports/2024-country-reports-on-human-rights-practices/panama>

¹⁶⁵Graña Gianoni, J. (April 2025). *Challenges to Freedom of Expression, the Rule of Law, and Democracy in Latin America: A Regional Study on SLAPPs*. Panama. Baltasar Garzón International Foundation (FIBGAR). <https://fibgar.es/wp-content/uploads/2025/04/Panama-Informe-Desafios-a-la-libertad-de-expresion-estado-de-derecho-y-democracia-en-latinoamerica-un-estudio-regional-en-tema-de-SLAPPs.pdf>

¹⁶⁶Inter-American Press Association. (July 4, 2024). *The IAPA welcomes the Supreme Court’s ruling that strengthens freedom of expression in Panama*. <https://www.sipiapa.org/comunicados-prensa/la-sip-saluda-fallo-la-corte-suprema-que-refuerza-la-libertad-expresion-panama-n1300679>

In the electoral arena, a package of reforms to the Electoral Code is currently under consideration. Submitted by the Electoral Tribunal to the National Electoral Reform Commission (CRNE)—which was established in February 2025—the package includes electoral offenses such as the dissemination of fake news and misinformation that may be “detrimental to the electoral process” or to the work of the Tribunal itself. By the end of November 2025, the work of the National Commission on Electoral Reforms was entering its final stretch, which will extend through January 2026. At that time, the Electoral Tribunal will be required to review, organize, and prepare a final package of proposals to be discussed in the National Assembly, which will decide the rules governing the upcoming elections in 2029.¹⁶⁷

8.3 Digital Environment

According to data collected from the ASEP’s Fixed Internet Service indicators, there is a steady upward trend in internet connectivity in Panama, evident in recent years; both the number of subscribers and the estimated total number of users have grown significantly during this period.

As shown in the table below, the penetration rate has risen from 13.9 subscribers per 100 inhabitants in 2020 to 17.3 in 2024. Meanwhile, user penetration rose from 48.3 in 2020 to 60 users per 100 inhabitants in 2024.

Table 8. Fixed Internet Service Indicators in Panama

Cuadro 1. INDICADORES DEL SERVICIO DE INTERNET FIJO EN LA REPÚBLICA. AÑOS 2020-24(e)

Indicador	2020	2021	2022	2023	2024(e)
Cientes de Internet	594,327	645,053	721,117	716,657	779,972
Residenciales	543,547	585,564	655,703	657,341	712,197
Comerciales	50,780	59,489	65,414	59,316	67,775
Cientes de Internet por cada 100 hab.	13.9	14.9	16.4	16.1	17.3
Cantidad de Clientes por tecnología	594,327	645,053	721,117	716,657	779,972
Cable Modem	515,368	518,905	673,399	665,667	736,433
xDSL	26,110	21,807	8,152	4,157	2,120
Wifi	3,477	6,248	4,829	8,094	7,195
Wimax	14,102	13,092	9,451	4,378	2,028
Otras Tecnologías (1)	35,270	85,001	25,286	34,361	32,196
Usuarios de Internet (2)	2,065,384	2,225,143	2,491,671	2,497,896	2,706,350
Usuarios de Internet por cada 100 hab.	48.3	51.3	56.7	56.1	60.0

(1) Otras tecnologías tenemos: ATM, Eternet, Frame Relay, MPLS, FFTx y Otras

(2) La cantidad de usuarios está basado en los clientes residenciales multiplicado por la cantidad de personas por hogar (Censo poblacional)

(e) Cifras estimadas

Fuente: Formulario de Información Técnica, Comercial y Estadística (FITCE)

www.asep.gob.pa | @AsepPanamá

Source: ASEP

Regarding digital literacy levels in the country, several reports¹⁶⁸ indicate that there is a huge gap in access to devices and connectivity between children in public schools and those in the private school

¹⁶⁷Gordón Guerrel, I. (November 22, 2025). *Electoral Reform Commission to Continue Through 2026*. La Estrella de Panamá. <https://www.laestrella.com.pa/panama/politica/comision-de-reformas-electorales-se-extendera-hasta-2026-GG17778817>

¹⁶⁸Cubilla-Bonnetier, D., Grajales-Barrios, M., Ortega-Espinosa, A., Puertas, L., & De León Sautú, N. (2023, February 6). *Unequal literacy development and access to online education in public versus private Panamanian schools during the COVID-19 pandemic*. *Frontiers in Education*, 8. <https://doi.org/10.3389/feduc.2023.989872>

system. Before the pandemic, only 40% of households with children attending public schools had internet access, and just 30% had a computer at home, compared to 90% and 80% of households with children in the private school system.

Meanwhile, another report focusing on college students,¹⁶⁹ shows that although all are social media users and most say they fact-check information, 10% of students admit they cannot identify reliable sources online, and most never cite the source when sharing others' information on social media—suggesting that critical digital literacy still needs to improve in the country.

Panama's PISA 2022 results¹⁷⁰ indicate that only 1% of students in Panama reached the highest levels in reading, suggesting that students are unable to distinguish facts from opinions based on content or sources. This is particularly concerning because it means that most 15-year-old students in Panama lack the reading skills necessary to detect misinformation.

The same report notes that approximately 20–24% of students reported being victims of *bullying* or harassment, a significant finding since such behaviors often occur in digital environments as well.

8.4 Digital platforms available in the country

In Panama, YouTube has about 2.73 million users in the country, a figure that continues to grow, while Instagram—which is also growing—is estimated to have about 2.70 million users in the country; in other words, they are equally popular, although Instagram's annual growth rate is lower. TikTok, however, has 3.18 million users aged 18 and older in Panama and is experiencing even greater growth, confirming its status as the most popular social media platform. Once again, Facebook and Twitter—now X—are popular, but they are not experiencing the same growth and lag far behind the top three in terms of user numbers.

If we look at the proportion of users reached by social media platforms in Panama, TikTok has the highest share at 80.4%, followed by YouTube (67.2%) and Instagram (73.4%), confirming that these are the three most popular social media platforms in the country. Facebook is right behind them, while Twitter and all the others lag far behind.¹⁷¹

Panama's digital ecosystem has been revitalized by the rapid growth of e-commerce and the widespread adoption of digital payment methods. In 2024, Panama recorded a historic high of 349 million electronic transactions, representing a year-over-year increase of 21 million transactions. Thus, the country's financial and technological inclusion is moving toward consolidation. According to data from Telered, the country's leading processor of transactions and low-cost payment methods, the volume of funds processed through these channels exceeded 108,900 million Balboas, driven by the widespread adoption of *the Clave System*—which processed up to 264, million transactions in a single year—and by the strong growth in instant transfers and the use of digital wallets.¹⁷²

8.5 Legislative and Regulatory Context in Panama

¹⁶⁹López de Ramos, A. L., Casado Robles, E., Atagua-Díaz, Z., Prado, J. F., Álvarez Franco, A. M., Cáceres, A., and Ramos Fortuna, V. (2024). *Analysis of digital literacy: Exploring the gender gap among Panamanian college students*. Latitude, 1(19), 22–46. <https://doi.org/10.55946/latitude.v1i19.242>

¹⁷⁰OECD. (2023). *PISA 2022 Results (Volume I): The State of Learning and Equity in Education*. OECD Publishing. <https://doi.org/10.1787/53f23881-en>

¹⁷¹Kemp, S. (2025, December 15). *Digital 2026: Panama*. DataReportal; Kepios. <https://datareportal.com/reports/digital-2026-panama>

¹⁷²Telered. (2025). News and updates on the electronic payment system in Panama. <https://www.telered.com.pa/category/teleres/>

8.5.1 Constitutional Framework

Panama's constitutional framework establishes a robust foundation for the protection of fundamental rights, which serves as a pillar for the regulation of digital environments. At its core, the Political Constitution of the Republic of Panama enshrines freedom of expression by stipulating that every person may freely express their thoughts verbally, in writing, or "by any other means," without being subject to prior censorship. This open-ended formulation allows constitutional protection to extend to the internet, digital platforms, and social media. However, the same constitutional text establishes that this right is not absolute, as it entails legal liabilities when, through its exercise, it infringes upon the reputation or honor of individuals, or in the case of acts that threaten social security or public order.

Furthermore, the Panamanian Constitution erects a strict barrier against arbitrary surveillance, a vital element for the safe exercise of journalism and freedom of expression in the digital age. It guarantees the inviolability of correspondence and private documents, expressly extending this protection to telephone communications and, by broad interpretation, to telecommunications and digital data. The constitutional mandate is clear in establishing that private communications may not be intercepted, recorded, or examined except by order of a competent judicial authority and in strict compliance with legal formalities. This guarantee protects users and the press from unlawful state interference in their electronic communications, safeguarding professional secrecy and the confidentiality of sources.

With regard to access to information and informational self-determination, the Panamanian Constitution incorporates modern and direct procedural tools, notably the concept of *habeas data*. Through this constitutional remedy, the right of every person to access information about themselves contained in public or private databases or records is recognized, as well as the right to demand its correction, updating, or confidentiality if such information is inaccurate or violates their rights. At the same time, the Constitution enshrines the right of access to public information, establishing the principle of maximum transparency that obligates the State to be transparent—a right that today is indispensably realized through open data portals and digital government platforms.

Finally, with regard to freedom of the press and democratic debate online, the Panamanian framework seeks a balance between prohibiting censorship and mitigating new digital risks. While the Constitution protects the media and prohibits their closure or expropriation as a means of silencing criticism, digital environments have introduced threats such as widespread disinformation and the use of *bots* and fake accounts, especially during election periods. As discussed in greater detail in the relevant section, Panama has amended its electoral legislation to address the realities of today's internet and the risks to electoral integrity.

8.5.2 Telecommunications and Media Legislation

The regulation of telecommunications and the media in the Republic of Panama is historically grounded in two fundamental pieces of legislation: Law 31 of 1996, known as the Telecommunications Law¹⁷³, and Law 24 of 1999, or the Broadcasting Law.¹⁷⁴ These laws were designed to organize the provision of services and comprehensively regulate the use of the radio spectrum, a public resource whose exploitation requires the granting of state concessions. Although these laws predate the

¹⁷³Panama. (February 9, 1996). *Law 31 of 1996: Establishing regulations for telecommunications in the Republic of Panama*. Official Gazette No. 22,971. https://www.gacetaoficial.gob.pa/gacetas/22971_1996.pdf

¹⁷⁴Panama. (June 30, 1999). *Law 24 of 1999: Regulating public radio and television services and establishing other provisions*. Official Gazette No. 23,832. (Updated with amendments and supplementary laws, including Law 281 of 2021). <https://asep.gob.pa/direcciones/telecomunicaciones/radio-y-television-digital/legislacion/>

widespread adoption of the internet and the emergence of digital platforms, they establish the principles of competition, state control, and protection of the public interest that underpin the country's current digital governance.

Law 24 of 1999 is particularly relevant due to its institutional design, as it designates the Public Services Regulatory Agency—currently the National Public Services Authority (ASEP)—as the entity with legal personality and its own assets, responsible for overseeing, regulating, and granting concessions in this sector. ASEP's role goes beyond mere technical administration; it has a mandate to safeguard the social welfare of citizens and ensure the promotion of competitive markets. This mission translates into oversight aimed at preventing practices that distort fair competition or harm investment in the country's communications infrastructure.

A provision in Law 24 of 1999 designed to protect democratic pluralism is the imposition of explicit restrictions intended to prevent media monopolies. The law prohibits cross-ownership between concessionaires of broadcast media (such as television and radio) and daily newspapers, seeking to prevent the concentration of public opinion in the hands of a few. Likewise, the law safeguards informational sovereignty by requiring that effective control of concessionary companies remain predominantly in the hands of Panamanian nationals, allowing exceptions only in the case of pay-TV or pay-radio services. Furthermore, this law laid the regulatory groundwork for the country's technological transition to digital radio and television.

With regard to the protection of the rights to information and freedom of the press, Decree 155 of 1962¹⁷⁵ stands out, as it regulates broadcasting in the country. In accordance with Article 37 of the Political Constitution of the Republic, Article 44 of this decree explicitly guarantees the free expression of thought without any form of prior censorship. This historic guarantee is intertwined with the Transparency Law (Law No. 6 of January 22, 2002),¹⁷⁶ which serves as a pillar for the practice of journalism and public scrutiny. This law guarantees the principle of public access to information and establishes mechanisms for active transparency and *habeas data*. At the same time, it classifies information, distinguishing between freely accessible information, confidential information (medical data, private life), and restricted-access information (national security, trade secrets), prohibiting the disclosure of the latter two categories while promoting citizen participation through public consultations prior to making administrative decisions that affect citizens' interests.

Law 59 of 2008 on Universal Service and Access to ICTs¹⁷⁷ seeks technological democratization and the reduction of the digital divide. This law aims to promote and guarantee access to information and telecommunications technologies throughout Panamanian territory, with a particular emphasis on providing coverage and quality to citizens with geographic or economic limitations. Article 2 elevates the right to communication and information to the level of a fundamental principle of universal service, alongside non-discrimination, transparency, and equity. Article 3 defines the right to information as the “fundamental guarantee that every person has to receive, seek, access, and disseminate information,” making this right a central component of freedom of expression in the context of access to technology.

To achieve these objectives, Law 59 establishes the creation of Funds for the Development of Service and Universal Access Projects, which are jointly financed by telecommunications operators through a surcharge applied to incoming international calls. Article 10 of the law stipulates that, when defining

¹⁷⁵Panama. (July 12, 1962). *Executive Decree No. 155 of July 12, 1962, regulating the practice of law and establishing the Code of Ethics and Professional Responsibility*. Official Gazette No. 14,672. <https://docs.panama.justia.com/federal/decretos-ejecutivos/155-1962-jul-12-1962.pdf>

¹⁷⁶Panama. (January 22, 2002). *Law No. 6 of 2002: Establishing rules for transparency in public administration, establishing the Habeas Data remedy, and enacting other provisions*. Official Gazette No. 24,476. https://www.gacetaoficial.gob.pa/gacetitas/24476_2002.pdf

¹⁷⁷Panama. (August 11, 2008). *Law No. 59 of 2008: Promoting universal service and access to information and telecommunications technologies for development and enacting other provisions*. Official Gazette No. 26,106. (Amended by Law No. 70 of 2009, Law No. 62 of 2012, and Law No. 197 of 2021). <https://www.gacetaoficial.gob.pa/pdfTemp/26106/12646.pdf>

projects (such as telemedicine or rural telecommunications), priority will be given to those that facilitate access to the “Knowledge Society,” recognizing that access to government information and citizen participation are non-negotiable goals. In addition, Article 20 mandates the modernization of existing infrastructure in hard-to-reach areas to enable internet connectivity.

In terms of rights protection, the Ombudsman’s Office of Panama plays a cross-cutting role. Created by Law No. 7 of 1997¹⁷⁸, this institution was elevated to constitutional status through the 2004 constitutional amendment, enshrining its functions and the requirements for the election of the Ombudsman in Articles 129 and 130 of the Constitution. The Ombudsman’s Office is tasked with ensuring the protection of the human rights of all the country’s inhabitants. Given its mandate to actively defend these rights against violations and to oversee the actions of the public administration, the institution possesses inherent legitimacy and authority to intervene in the protection of the rights of users and citizens in the increasingly complex digital sphere.

8.5.3 Specific Regulation on Platforms and/or Content Regulation

To date, Panama has not enacted a law that explicitly refers to the “regulation of digital platforms” or “content moderation.” However, the country has a regulatory framework for the internet and its services that operates in a similar manner, although it is clear that modernization is needed to enable it to address the current challenges of digital environments more effectively—particularly as these environments have evolved with the emergence of major digital platforms.

Law No. 51 of July 22, 2008,¹⁷⁹ “which defines and regulates electronic documents and electronic signatures, as well as the provision of technological document storage services and electronic signature certification, and adopts other provisions for the development of e-commerce,” contains provisions that go beyond commerce and establishes the fundamental legal framework for business, digital transactions, the obligations of internet intermediaries, and is therefore of particular relevance to platform governance.

The broad scope of Law No. 51 is evident from Article 2, which defines the regulated entities. The law categorizes as “intermediation service providers” not only internet service providers (ISPs) or telecommunications networks, but also those who provide temporary or permanent data storage services (cloud services and *hosting*), and, crucially, those who provide “tools for searching, accessing, and collecting data or links to other websites.” This broad definition can be interpreted to include search engines, content aggregators, and current social media platforms, serving as a legal basis for holding them accountable under the Panamanian framework and providing elements useful for the regulation of digital platforms.

Article 3 of this same law stipulates the guiding principles of digital services, including freedom of provision, compatibility, equivalence, and technological neutrality. However, it imposes clear limits, establishing that the activities of service providers must comply with the provisions of other laws regarding the protection of public health, national security, personal data, and consumer interests. Likewise, Title VI of the law, which regulates e-commerce over the internet, introduces territoriality criteria in Articles 77 and 78. A company is considered to be established in Panama if it centralizes its administrative management in the country or has logistical support facilities there. More importantly, Article 78 stipulates that foreign companies selling goods or services online to Panama

¹⁷⁸Panama. (February 5, 1997). *Law No. 7 of February 5, 1997, establishing the Office of the Ombudsman*. Official Gazette No. 23,222. (Partially superseded and supplemented by Law 504 of 2024). <https://www.defensoria.gob.pa/books/ley-no-7-de-5-de-febrero-de-1997-por-la-cual-se-crea-la-defensoria-del-pueblo/>

¹⁷⁹Panama. (July 22, 2008). *Law No. 51 of 2008: Defining and regulating electronic documents and electronic signatures, as well as the provision of document storage and electronic signature certification services, and adopting other provisions for the development of e-commerce*. Official Gazette No. 26,090. (Amended by Law No. 82 of 2012). https://www.gacetaoficial.gob.pa/gacetitas/26090_2008.pdf

must comply with the technical and legal requirements in force in the country, paving the way for transnational platforms to be subject to local legislation that protects citizens' rights.

The most significant aspect of Law 51 regarding the regulation of platforms is the establishment of a "liability exemption regime," detailed in Chapter III. While Article 84 subjects service providers to general civil, criminal, and administrative liabilities, Articles 88 through 91 establish safeguards. They stipulate that intermediaries, network operators, and access providers are not liable for the information they transmit if they did not initiate the transmission, do not modify the data, and do not select the recipients. This immunity covers automatic and temporary storage (*caching*), provided that the platform diligently removes the information upon learning that it has been removed from the original source.

The core of this regime rests on the concept of "actual knowledge." Providers of data *hosting*, links, and search tools are exempt from all liability for unlawful or harmful content stored by third-party users, provided they have no actual knowledge of such unlawfulness. Platforms are only liable if, after acquiring such knowledge (for example, through formal notification or a ruling by a competent authority), they fail to act with due diligence to remove the data or disable access to it. This legal model means that, in Panama, platforms do not have a general obligation to proactively monitor or filter all content circulating on their networks in order to maintain their immunity, thereby establishing a system of reactive collaboration similar to that in place in the United States and the European Union.

The administrative authority empowered to oversee this ecosystem is the General Directorate of Electronic Commerce (DGCE), which is attached to the Ministry of Commerce and Industry. Its powers are defined in multiple articles (including Articles 69 through 71, 80, 81, and 95 through 97, among others). The DGCE has inspection powers: it conducts technical audits, administers the registry of storage service providers, and may impose severe sanctions, including the suspension or "permanent ban" of services for repeat offenders (Articles 63 and 101)—a measure that could be problematic without appropriate limits. It also has quasi-judicial authority: Articles 95–97 grant it standing to initiate suspension proceedings against acts contrary to the law, either on its own initiative or at the request of affected third parties (such as consumer associations).

The DGCE's powers are directly linked to content moderation. According to Articles 83 and 87, any competent authority that determines that content violates public order, public health, human dignity, or consumer protection does not directly order the intermediary to block the content, but must instead submit a reasoned request to the DGCE. Upon granting the request, the DGCE becomes the authority responsible for ordering local internet service providers to suspend transmission or block access to data, including that from foreign providers. To ensure compliance, Article 102 empowers the DGCE to impose fines for noncompliance that may amount to 5% of the original penalty for each day of noncompliance. Aware of the weight of these measures, the legislature included safeguards in Articles 39, 65, 83, and 103, requiring that any restrictive measure be objective, proportionate, and guarantee absolute respect for fundamental rights such as privacy and freedom of expression.

To complement government oversight, Panamanian law relies on co-regulation. Articles 92 through 94 empower the DGCE to promote the creation of voluntary codes of conduct at the national level. These codes, which become binding on those who adopt them, must be developed with the participation of consumers and users. Their relevance for platforms is significant, as they allow for the development of standardized procedures for detecting and removing illegal content, protecting against *spam*, and establishing out-of-court dispute resolution mechanisms. Executive Decree 24 of 2019, which regulates Law 51, implements this in Chapter VII by creating a system of "trust seals" for companies that adopt these codes, requiring them to incorporate privacy standards, child protection measures, and transparent systems for resolving user complaints.

Finally, Law No. 44 of October 10, 2012, on Copyright and Related Rights¹⁸⁰ is also of great relevance to the digital environment. This law modernized Panama's legal framework to encompass the internet, stipulating in Articles 2 and 55 that making works available to the public includes digital networks and on-demand *streaming*. Software and databases are also protected (Articles 22 and 33). Title XI of the law defines "technological compliance" offenses, severely penalizing the circumvention of technological self-protection measures (DRM locks) and the alteration of rights management information (RMI). Of particular relevance to platforms is Article 158, which grants the General Directorate of Copyright the administrative authority to order the immediate suspension of any unauthorized public communication or digital transmission, seize equipment, and order blocking measures when exploitation licenses are not provided, thereby having a significant impact on the removal of protected content from the internet.

8.5.4 Data Protection and Privacy Legislation

The right to privacy and the processing of citizens' personal information in Panama are regulated by Law 81 of 2019 on the Protection of Personal Data¹⁸¹. This law establishes the general and mandatory legal framework for the processing of personal data, covering both private-sector companies and public-sector entities, with a particular emphasis on informational self-determination.

Law 81 is based on guiding principles detailed in Article 2. Among these, the principles of fairness and lawfulness stand out, requiring transparency from the outset. It also establishes the principles of purpose and proportionality, which stipulate that data controllers may only collect data that is strictly necessary for a specific, legitimate, and explicit purpose, prohibiting any subsequent processing that is incompatible with the original purpose. Also fundamental is the principle of security and confidentiality, which legally obligates data controllers to implement robust technical and organizational measures to protect information against unauthorized access, alteration, or loss, and to maintain strict professional secrecy.

To legitimize the processing of personal data, Article 6 of the law establishes as a general and indispensable rule the requirement to obtain the data subject's prior, informed, and unambiguous consent. Exceptions are limited to those specifically provided for by law in Article 8, such as the performance of a contract to which the data subject is a party, compliance with legal obligations imposed on the controller, situations of imminent medical emergency, or when the data comes from sources with unrestricted public access. This strict regulatory framework extends to cross-border data flows. Article 5 prohibits the transfer of data to third parties, both domestically and internationally, without the user's consent, unless the receiving country or the receiving entity offers protection and security standards equivalent to those required by Panamanian law, or unless there are international treaties on cooperation and the prosecution of crimes that justify such a transfer.

Article 15 legally enshrines the ARCO rights: the right of Access to know what personal data is being processed; the right of Rectification regarding inaccurate or incomplete data; the right of Cancellation (deletion) of data whose processing does not comply with the law or whose purpose has expired; and the right of Objection to processing on legitimate grounds. In an innovative move, the right to data portability is added to these traditional rights. This legal guarantee empowers users to request and obtain a complete copy of their personal data structured in a generic, commonly used electronic format, allowing them to operate across different digital ecosystems without losing their history or profiling.

¹⁸⁰Panama. (October 10, 2012). *Law No. 44 of 2012: Establishing rules on copyright and related rights and setting forth other provisions*. Official Gazette No. 27,141. https://www.gacetaoficial.gob.pa/gacetitas/27141_2012.pdf

¹⁸¹Panama. (March 26, 2019). *Law No. 81 of 2019: On the Protection of Personal Data*. Official Gazette No. 28,743-A. https://www.gacetaoficial.gob.pa/gacetitas/28743A_2019.pdf

The institutional framework responsible for ensuring compliance with this law is led by the National Authority for Transparency and Access to Information (ANTAI). Through the powers granted in Articles 7, 17, and 36, ANTAI serves as the governing body and national supervisory authority, with full authority to monitor databases, initiate investigations on its own initiative or in response to citizen complaints, and impose the corresponding sanctions. To strengthen the democratic governance of privacy, Article 34 establishes the Data Protection Council. This multisectoral advisory body includes representatives from the government, private business associations, and professional associations, and is tasked with providing specialized technical advice to ANTAI and recommending the design of relevant public policies.

8.5.5 Specific Regulations for the Protection of Vulnerable Groups

The Panamanian government has developed a specific criminal and institutional framework designed to protect the most vulnerable populations from threats that have intensified through the use of information and communication technologies. The Penal Code (consolidated text of 2019)¹⁸² incorporates international human rights treaties in Article 5 and has been amended to address cybercrime, reinforced by Law 79 of 2013¹⁸³, which incorporates the provisions of the Budapest Convention. This latter law is vital because Article 12 establishes the liability (criminal, civil, or administrative) of legal entities—including companies and platforms—when cybercrimes are committed by executives or subordinates due to negligence or a lack of oversight within the entity.

The protection of minors in the digital environment is addressed with extreme rigor in the Penal Code. Article 184 criminalizes child sexual exploitation, imposing severe penalties of 10 to 15 years in prison on anyone who produces, publishes, or distributes child pornography via the internet or any other mass media. The law provides for specific aggravating circumstances that increase the prison sentence by an additional 5 years if the victim is under 14 years of age or if it is proven that the exploitation of the illicit material was for profit.

Furthermore, Panamanian law addresses cyberbullying and predatory online tactics known as “grooming.” Article 187 is designed to punish the strategies that abusers use to gain the trust of minors for the purpose of sexual exploitation. This article imposes prison terms of 8 to 10 years on individuals who use email, social media platforms, messaging apps, or other means of communication to incite minors to engage in sexual acts or to promote such services. Along the same lines of protection, Article 190 criminalizes the promotion or advertising of sex tourism through any medium, including the digital space, establishing sentences ranging from 10 to 12 years in prison.

In the area of protecting women and combating gender-based violence, Panama took a historic legislative step with the enactment of Law 82 on October 24, 2013.¹⁸⁴ This comprehensive law adopts preventive measures against violence and amends the Penal Code to introduce the criminal offense of femicide. Article 3 defines violence against women in a broad manner, including discriminatory practices in both the public and private spheres. What is truly groundbreaking for the digital ecosystem is Article 4, paragraph 21, which defines and introduces the concept of “media violence.” This is described as the publication or dissemination, through any mass medium, of stereotypical messages and images that promote exploitation, that insult, dishonor, or humiliate women, or that legitimize unequal treatment and reinforce sociocultural patterns that perpetuate violence.

¹⁸²Panama. (May 14, 2019). *Penal Code of the Republic of Panama* (Consolidated Text published in the Official Gazette No. 28,774-B). https://www.gacetaoficial.gob.pa/gacetass/28774B_2019.pdf

¹⁸³Panama. (November 14, 2013). *Law No. 79 of 2013: Approving the Convention on Cybercrime, done at Budapest on November 23, 2001*. Official Gazette No. 27,415. https://www.gacetaoficial.gob.pa/gacetass/27415_2013.pdf

¹⁸⁴Panama. (October 24, 2013). *Law No. 82 of 2013: Adopting preventive measures against violence against women and amending the Penal Code to criminalize femicide and punish violence against women*. Official Gazette No. 27,401. https://www.gacetaoficial.gob.pa/gacetass/27401_2013.pdf

Law 82 itself recognizes the digital dimensions of abuse through its definition of “sexual violence,” which explicitly includes the recording or dissemination without consent of intimate images through any medium. The Penal Code penalizes the dissemination—without consent or proper authorization—of private recordings, images, or documents that were not intended for public release.

Although Panama does not have a law or criminal offense that generally punishes “hate speech,” the legal system punishes hostile expressions online when they cross the line into incitement to violence, systematic discrimination, or defamation. Article 178 imposes criminal penalties on anyone who sexually harasses, intimidates, or discriminates against a person in work or educational settings, paving the way for its application when these acts occur in corporate or school digital environments. Furthermore, the penalties for the traditional crimes of defamation and slander (Articles 193 through 195) have been substantially increased, with penalties potentially including actual prison terms when offenses against dignity, honor, or decorum—or the false attribution of a crime—are committed on a massive scale “using a computer system” or through social media.

Finally, to safeguard the public’s security against extreme online threats, the Penal Code criminalizes cyberterrorism. Article 293 establishes that the use of “cyber means” to commit acts of terrorism intended to cause panic or a common danger to the public will be punishable by extremely severe sentences of 20 to 30 years in prison. As a preventive measure, Article 295 criminalizes online terrorist instruction, imposing a prison term of 5 to 10 years on anyone who uses internet platforms to teach how to build explosive devices or to actively recruit individuals for acts of terror, thereby imposing an absolute legal limit on freedom of expression when it is used to incite the commission of atrocities.

8.5.6 Digital Electoral Regulation

The electoral regulatory framework is codified in the Consolidated Text of the Electoral Code of 2022.¹⁸⁵ The code incorporates the reforms introduced by Law 247 of October 2021¹⁸⁶, establishing an electoral justice framework designed to adapt to the digital environment. The code comprehensively regulates the structure of the Electoral Tribunal, the Office of the Electoral Attorney General, political rights, and campaign financing.

The Panamanian Electoral Code explicitly recognizes and regulates “digital media” as official channels for the dissemination of political propaganda. Articles 260 and 262 include within this legal definition the internet in general, social media, mobile applications, search engines, and mass messaging services. By regulating these media, the law subjects digital political messaging to the same standards as traditional campaign advertising.

Article 276 establishes strict prohibitions to which all online election campaigns are subject, strictly forbidding “smear campaigns.” This is legally defined as content that offends human dignity through insults, constitutes slander, invades privacy, promotes systematic discrimination, or alleges the commission of illegal acts that have not been previously ruled upon and proven by courts of law.

To prevent shadow financing and the manipulation of algorithms through illicit funds, Article 213 requires all pre-candidates, candidates, and political parties to grant the Electoral Tribunal direct access to the advertising management tools on their social media accounts and platforms. The objective is to enable real-time audits and technical monitoring of advertising spending; any advertising that evades this monitoring is excluded for the purposes of reimbursement of public election funding. Articles 287 through 290 require political actors to register with the Electoral Tribunal

¹⁸⁵Panama. (February 15, 2022). *Electoral Code of the Republic of Panama* (Consolidated Text published in Official Gazette No. 29,482-A of February 22, 2022).

<https://www.gacetaoficial.gob.pa/pdfTemp/29482A/89751.pdf>

¹⁸⁶Panama. (October 22, 2021). *Law No. 247 of October 22, 2021, amending the Electoral Code of the Republic of Panama*. Official Gazette No. 29,403-A.

https://www.gacetaoficial.gob.pa/pdfTemp/29403_A/GacetaNo_29403a_20211022.pdf

the official URLs of their websites, institutional and paid accounts, and to fully identify the administrator or agency responsible for managing their digital media. Furthermore, all digital advertising must prominently display a transparency banner or label.

The Electoral Code also addresses the threats posed by automated disinformation. Article 292 contains specific provisions against mass manipulation in digital media, imposing severe penalties for the use of centers housing inauthentic accounts (profile farms) and the use of *bots* designed to alter the electorate's perception. The Electoral Tribunal, through its National Directorate of Electoral Organization, has the authority to verify and identify those responsible and to order the immediate administrative suspension of these toxic campaigns. Once administrative remedies have been exhausted, the law requires that the case be referred to the Electoral Attorney General's Office.

Decree No. 7 of January 23, 2024¹⁸⁷ adds a chapter to the Electoral Code whose sole purpose is to regulate and combat mass manipulation of digital media aimed at undermining the integrity of the electoral process. Article 1 provides legal definitions of modern concepts such as "electoral disinformation" and "mass manipulation." Article 2 sets forth a detailed list of twenty prohibited acts that constitute such manipulation, adapting the law to the risks of the 21st century. The decree prohibits the malicious use of artificial intelligence to create *deepfakes* (altered images, audio, or video); the use of click farms to amplify harmful propaganda; harassment aimed at silencing political opponents or minorities; and the use of micro-targeting techniques designed to disseminate false messages. The decree empowers any citizen and the Electoral Tribunal itself to report the dissemination of fake news through closed messaging apps (such as WhatsApp) or the manipulation of search engines, ensuring that the tools for defending democracy are aligned with technological realities.

Panama's electoral authorities have promoted the signing of the Digital Ethics Pact, a voluntary instrument that calls on political parties, candidates, media outlets, digital agencies, and *influential* citizens to make a public commitment to decency in cyberspace. The pact's signatories assume the civic duty to respect legal campaign windows (campaign blackout periods), expressly renounce the use of "smear campaigns," *bots*, and fake accounts to undermine reputations, and commit to playing a proactive role in educating their audiences, verifying the authenticity of audiovisual materials before sharing them (especially given the rise of generative AI), and fostering an environment for political debate where the exchange of ideas takes precedence over systematic digital harassment.

8.6 Alignment with UNESCO Guidelines: Panama

An analysis of Panama's regulatory framework, compared with the UNESCO Guidelines for the Governance of Digital Platforms, reveals a regulatory ecosystem with solid constitutional foundations and notable sectoral progress, but one that still requires systemic modernization to regulate internet intermediaries through a comprehensive human rights-based approach.

Fundamentally, Panama demonstrates positive alignment regarding the protection of human rights and freedom of expression; the Constitution prohibits prior censorship in a technology-neutral manner and erects strict barriers against arbitrary surveillance, always requiring a court order to intercept private communications. In terms of data architecture, Law 81 of 2019 establishes a robust model for privacy and data protection and delegates its oversight to a specific authority (ANTAI), which is in line with the protection of autonomy promoted by UNESCO.

¹⁸⁷Panama. (January 23, 2024). *Executive Decree No. 7 of January 23, 2024, regulating Law No. 81 of March 26, 2019, on the Protection of Personal Data*. Official Gazette No. 29,956-B. https://www.gacetaoficial.gob.pa/pdfTemp/29956B/GacetaNo_29956b_20240125.pdf

Regarding the regulation of platforms and the content ecosystem, the country does not have a modern law that specifically regulates the governance of social media. Instead, it relies on Law 51 of 2008 (on e-commerce and electronic documents), which establishes a liability exemption regime similar to the “safe harbor” model. This law stipulates that platforms are not liable for third-party content unless they have “actual knowledge” of its illegality and fail to act diligently to remove it. Although this approach avoids proactive censorship and, in principle, aligns with international standards of proportionality, the designation of the General Directorate of Electronic Commerce (DGCE) as the authority empowered to order administrative blocks—which could lead to permanent bans—raises serious concerns. This institutional design represents a critical gap with respect to UNESCO’s recommendation to establish an independent regulator specialized in mitigating human rights risks and separate from purely commercial or direct governmental spheres; in other words, there is a clear opportunity for improvement.

Where Panama demonstrates remarkable alignment is in its response to threats to electoral integrity in the digital environment. The Electoral Tribunal has spearheaded reforms to the Electoral Code (such as Law 247 of 2021 and Decree No. 7 of 2024) that directly address the systemic risks identified by UNESCO. Panamanian legislation requires transparency in the financing of digital advertising, strictly prohibits mass manipulation through the use of *bots* and bot farms, and, in a pioneering move, criminalizes the malicious use of artificial intelligence (*deepfakes*) for electoral disinformation. In addition, the government complements punitive regulation with self-regulatory tools and civic engagement initiatives, such as the Digital Ethics Pact, fostering shared responsibility among political actors, the media, and citizens in building a healthy information ecosystem.

Even so, significant gaps remain that limit the effective protection of public deliberation. While UNESCO insists on decriminalizing expression and prioritizing civil sanctions, serious problems of judicial harassment against journalists persist in Panama, often taking the form of SLAPPs (Strategic Lawsuits Against Public Participation) based on criminal laws against libel and slander that carry prison sentences, which are aggravated if committed via social media.

Finally, although Law 59 of 2008 promotes universal access to ICTs, digital empowerment remains an unfulfilled goal; alarming international educational indicators reveal that the vast majority of Panamanian students lack the reading comprehension necessary to distinguish between facts and opinions, leaving the population highly vulnerable to misinformation and creating an urgent need for the implementation of aggressive national policies on media and information literacy.

9. Country Analysis: Dominican Republic

9.1 Political and Legal System

The regulatory and political framework of the Dominican Republic is structured under a democratic, presidential system of government, based on the classic separation of three independent branches: the executive, legislative, and judicial, which coexist with various autonomous constitutional oversight bodies. All of this is established in the country's Constitution.¹⁸⁸

The executive branch is headed by the Presidency of the Republic and operates through a network of ministries and government agencies. The legislative function, meanwhile, rests with the National Congress, a bicameral body composed of the Senate and the Chamber of Deputies, which has exclusive authority to propose, debate, and approve the country's laws.

In the area of the administration of justice and the defense of the rule of law, the system is structured primarily around the Supreme Court of Justice and the Constitutional Court. The latter, established following the 2010 constitutional reform, acts as the supreme interpreter and ultimate guarantor of constitutional supremacy. At the same time, the authority to initiate public criminal proceedings and the strategic direction of criminal policy rest with the Attorney General's Office.

In electoral matters, the administration and logistics of elections are the responsibility of the Central Electoral Board (JCE), whose operational functions were recently strengthened by the entry into force of a new Organic Law on the Electoral System in 2024. In turn, judicial review and the resolution of disputes in this area fall under the jurisdiction of the Superior Electoral Court (TSE), thereby ensuring a system of checks and balances in the electoral cycle.

At the territorial level, the Dominican Republic is administratively organized into provinces, the National District, and municipal districts—which include municipal districts—operating under local governments composed of mayors and municipal councils elected by direct popular vote. However, despite this regulatory framework, the formal decentralization model faces significant operational and structural challenges. As observed in other countries in the region, territorial autonomy clashes in practice with marked limitations on the financial and administrative capacity of municipal governments to effectively exercise their powers and address citizens' demands.

9.2 Freedom of Expression and Human Rights

The Dominican Republic's constitutional framework expressly recognizes freedom of expression and access to information as fundamental rights, and the law provides procedural mechanisms for their protection. In practice, however, the effective status of these rights is shaped by a confluence of legal, institutional, and contextual factors: protection of the press, independence of oversight bodies, and accountability of public authorities.

¹⁸⁸Dominican Republic. (June 13, 2015). *Constitution of the Dominican Republic*. Proclaimed on June 13, 2015. Official Gazette No. 10,805.

The Dominican Republic has a multi-level protection framework, based on Article 49 of the Constitution and the General Law on Free Access to Public Information (Law 200-04).¹⁸⁹ Unlike in other contexts, the Constitutional Court has developed case law on Habeas Data, allowing citizens to control the use of their personal data, although the application of the “right to be forgotten” remains a subject of doctrinal and jurisprudential debate in light of the public interest in information.

International assessments show that the Dominican Republic maintains relatively favorable rankings in regional comparisons. Independent reports, such as that by Reporters Without Borders (RSF), place the country in the upper-middle tier of the World Press Freedom Index. Such reports have highlighted the issue of economic pressures affecting the practice of journalism. Between 2024 and 2025, there was a slight decline in the national score. However, for the 2023–2024 period, reports from RSF and the Inter-American Press Association (IAPA) have warned of a deterioration in safeguards for the practice of journalism.¹⁹⁰ Although the country has maintained relatively high rankings in global indices, situations related to the digital security of journalists have been documented.

Table 9. Dominican Republic’s Scores and Rankings in Freedom of Expression Indices

Report or Index	Rating	Rank	Year
Reporters Without Borders	69.87	43	2025
V-Dem	0.9	28	2024

Source: Author’s own calculations based on RSF (2025) and V-Dem (2024).

Human rights organizations and international reports agree on specific problems: incidents of threats against journalists, instances of interference with access to information, and risks stemming from media concentration and the economic fragility of media outlets.

In the case of reports by Human Rights Watch and the U.S. Department of State, it has been noted that certain indirect restrictions and specific government practices may be emerging that could reduce the space for investigative journalism and criticism¹⁹¹. Likewise, significant public events (such as controversial legislative proposals and journalist protests in 2025) have reignited the debate on the risk of regulatory measures that could lead to censorship or undue control over digital content. These events do not necessarily imply a policy of widespread censorship, but they highlight the vulnerability of freedom of expression in the face of regulatory measures that require special attention.

A recent turning point was the finding by Amnesty International, in collaboration with the Security Lab, which confirmed the use of Pegasus spyware against investigative journalist Nuria Piera¹⁹². This incident revealed the vulnerability of the private communications of those investigating corruption and exposed the lack of effective controls over state intelligence agencies.

Furthermore, the regulatory climate became significantly more tense with the enactment of Law 1-24¹⁹³, which established the National Intelligence Directorate (DNI) in early 2024. Both civil society

¹⁸⁹ Dominican Republic. (July 28, 2004). *General Law on Free Access to Public Information (Law No. 200-04)*. Official Gazette No. 10,290.

¹⁹⁰ Reporters Without Borders, *2024 World Press Freedom Index: Dominican Republic* (Paris: RSF, 2024), <https://rsf.org/es/pais/republica-dominicana>.

¹⁹¹ Reporters Without Borders. (2025). *2025 World Press Freedom Index: Dominican Republic*. <https://rsf.org/en/index>

¹⁹² Amnesty International. (May 2, 2023). Dominican Republic: The discovery of Pegasus spyware on a prominent journalist’s phone must lead to an impartial investigation. <https://www.amnesty.org/es/latest/news/2023/05/dominican-republic-discovery-of-pegasus-spyware-on-prominent-journalists-phone/>.

¹⁹³ Dominican Republic. (2024, January 15). *Law No. 1-24 establishing the National Intelligence Directorate (DNI) and the National Intelligence System (SNI)*. Official Gazette No. 11,156.

and the Dominican Journalists' Association (CDP) denounced that the ambiguity of this law could force journalists and private companies to hand over confidential information to the state without a prior court order, thereby violating professional secrecy and the protection of sources.¹⁹⁴

According to RSF's analysis, most traditional media outlets are controlled by a small number of business groups, which encourages self-censorship on issues that could affect the economic interests of these conglomerates.¹⁹⁵ Unlike the direct physical violence observed in other Central American countries, situations in the Dominican Republic involve threats related to civil litigation and incidents of digital harassment. Unlike the conclusions reached in these reports on other Central American countries, in the case of the Dominican Republic, concerns have been raised about potential instances of state digital surveillance and the use of legislation on high-tech crimes (Law 53-07)¹⁹⁶ to investigate criticism on social media.

Institutionally, the protection of this set of rights depends on several bodies: the Constitutional Court and the Supreme Court for judicial protection, the Central Electoral Board for matters related to campaign advertising during elections, and administrative entities that regulate media and infrastructure (INDOTEL). As is the case in other Central American countries, constitutional case law¹⁹⁷ regarding access to information and freedom of expression has also provided a legal avenue that highlights the essential nature of these rights and sets limits on administrative actions.

9.3 Digital Environment

The Dominican digital landscape has experienced sustained growth in recent years, resulting in high internet penetration rates and widespread adoption of social media. Data from 2025 shows that at least 90% of the population is connected to the internet, with figures ranging from 88.6% to 91% across various reports, placing the Dominican Republic among the most connected countries in the region¹⁹⁸.

This level of connectivity is accompanied by widespread availability of mobile subscriptions: active cellular connections exceed 90% of the population, which explains the central role of mobile devices in the distribution and consumption of information. All of this has direct implications for the governance of digital platforms and the dissemination of content (including the phenomenon of disinformation), as the high level of penetration also implies a high degree of susceptibility or exposure to information disruptions via digital channels.

Regarding social media use, data from 2025 indicate that between 60% and 70% of the population maintains active accounts on social media platforms, with variations by platform and age.¹⁹⁹

From a public policy perspective, the growth in connectivity has driven government and private initiatives aimed at digital inclusion, but it also poses challenges related to infrastructure (quality and

¹⁹⁴ Inter-American Press Association. (April 2024). *Dominican Republic Report to the Mid-Year Meeting*. <https://www.sipiapa.org/notas/1216584-republica-dominicana>.

¹⁹⁵ Reporters Without Borders. (2023). *Dominican Republic: Economic Context*. In World Press Freedom Index 2023., <https://rsf.org/es/pais/republica-dominicana>.

¹⁹⁶ Dominican Republic. (April 23, 2007). *Law No. 53-07 on High-Tech Crimes and Offenses*. Official Gazette No. 10,416.

¹⁹⁷ Constitutional Court of the Dominican Republic. (October 22, 2012). Ruling TC/0042/12. Constitutional Court of the Dominican Republic. (February 19, 2016). Ruling TC/0075/16. Constitutional Court of the Dominican Republic. (May 19, 2020). Ruling TC/0175/20. Constitutional Court of the Dominican Republic. (July 18, 2022). Ruling TC/0249/22.

¹⁹⁸ Kepios / DataReportal, Digital 2025: The Dominican Republic (mobile penetration and connection statistics). <https://datareportal.com/reports/digital-2025-dominican-republic>

¹⁹⁹ Kepios / DataReportal, Digital 2025: The Dominican Republic (mobile penetration and connection statistics). <https://datareportal.com/reports/digital-2025-dominican-republic>

speed), media literacy, and platform regulation. Available data²⁰⁰ suggests that the physical availability of connectivity is no longer the main limitation; rather, attention appears to be needed on other factors such as service quality, affordable access, data protection, and strengthening citizens' critical skills to address information disruptions.

9.4 Digital Platforms Available in the Country

The Dominican market features the usual array of social media platforms and digital services that dominate the region: Facebook (and Messenger), Instagram, WhatsApp, YouTube, TikTok, and X (formerly Twitter), along with local news services and aggregators. Usage patterns show that Meta's platforms (Facebook/Instagram/Messenger/WhatsApp) maintain a leading position in terms of reach and time spent on the platforms, with Instagram and Facebook reporting several million active users and significant advertising reach; YouTube remains the primary repository for long-form audiovisual content; and TikTok has grown primarily due to its use among younger demographics.

From a commercial perspective, the digital advertising ecosystem in the Dominican Republic relies heavily on the global infrastructure of intermediaries (platforms that act as advertising marketplaces), which hinders the traceability of political spending and fiscal oversight of cross-border advertising. Market reports and fact sheets from DataReportal²⁰¹ show that audiences are concentrated on a few platforms.

9.5 Legislative and Regulatory Context in the Dominican Republic

9.5.1 Constitutional Framework

Like other examples of recent Latin American constitutionalism, the Dominican constitutional framework²⁰² establishes fundamental principles and rights related to freedom of expression, access to public information, and the confidentiality of communications.

The Dominican constitutional framework grants international human rights treaties a higher hierarchical status within the constitutional hierarchy (Article 74.3), which obligates public authorities to interpret national laws in accordance with the American Convention and other international instruments. The legislature retains the authority to regulate the exercise of these rights, while the Executive Branch, through the Dominican Telecommunications Institute (Indotel), administers the radio spectrum, which is recognized by Article 14 of the Constitution as an inalienable asset of the Nation.

With regard to freedom of expression and of the press, Article 49 of the Dominican Constitution enshrines the fundamental right of every person to freely express their thoughts, ideas, and opinions by any means, expressly prohibiting the establishment of any form of prior censorship. This article details the rights inherent to freedom of the press and freedom of information: it guarantees the right to seek, investigate, receive, and disseminate information of a public nature, and ensures that the media have free access to official and private news sources of public interest. As a vital safeguard for

²⁰⁰ Kepios / DataReportal, Digital 2025: The Dominican Republic (mobile penetration and connection statistics). <https://datareportal.com/reports/digital-2025-dominican-republic> Republic (see updates and figures on internet penetration, social media users, and mobile connections),

²⁰¹ Kepios / DataReportal, Digital 2025: The Dominican Republic (mobile penetration and connection statistics). <https://datareportal.com/reports/digital-2025-dominican-republic> (see updates and figures on internet penetration, social media users, and mobile connections),

²⁰² Dominican Republic. (June 13, 2015). *Constitution of the Dominican Republic*. Proclaimed on June 13, 2015. Official Gazette No. 10,805.

the free exercise of journalism, the Dominican Constitution explicitly protects professional secrecy and the journalist's right to refuse to disclose information on grounds of conscience, while also recognizing the public's right to reply and correction. These freedoms, however, are not absolute; their exercise is subject to constitutional limits regarding respect for the right to honor, privacy, dignity, and morality, with a particular emphasis on the protection of youth and children.

In the realm of digital rights, the secrecy of communications, and privacy, the 2010 Constitution represents a significant advance by incorporating modern technological language. Article 44, dedicated to the right to privacy and personal honor, formally recognizes the inviolability of correspondence, documents, or private messages expressly in “physical, digital, electronic, or any other format.” Likewise, it directly safeguards the confidentiality of “electronic, telematic, or other forms of communication,” stipulating that such communications and metadata may only be seized, intercepted, or recorded pursuant to a reasoned order from a competent judicial authority, while always preserving the confidentiality of private information unrelated to the investigation.

Alongside the privacy of communications, the Dominican Constitution establishes safeguards for data protection in the information age. Article 44 itself recognizes the right of individuals to access data about themselves held in official or private records, requiring that the processing of such personal information respect the principles of “quality, lawfulness, fairness, security, and purpose.” This protection is procedurally enshrined through the *Habeas data* remedy (Article 70), empowering citizens to access their data and to demand the suspension, rectification, updating, and confidentiality of such data in the event of inaccuracy or discrimination. Of particular relevance is the cross-protection afforded to the press in this area: by establishing the *Habeas Data* remedy, the Constitution imposes a categorical prohibition by stating that “the confidentiality of journalistic sources shall not be compromised,” thereby achieving a balanced coexistence between the protection of privacy in the digital environment and the essential safeguards for investigative journalism.

Furthermore, the constitutional text is not limited to the passive protection of these rights but imposes active obligations on the State to democratize the public sphere and the information environment. Paragraph 5 of Article 49 requires that the law guarantee “equitable and pluralistic access for all social and political sectors to State-owned media.” This inclusive vision is reinforced in Article 63, concerning the right to education, which imposes on the media the responsibility to contribute to civic education and emphasizes that the State must guarantee public radio and television services and “library and computer networks,” with the explicit purpose of enabling “universal access to information.”

However, the exercise of freedom of expression—and by extension, that of the press and civic activity in digital environments—is subject to an extraordinary limitation dictated by the Dominican Republic's own Constitution: Article 266 authorizes the temporary suspension of the right to freedom of expression and the inviolability of correspondence and communications during the declaration of states of internal unrest and emergency. This suspension, however, seeks to maintain a minimum level of guarantees, since states of exception must be duly justified, authorized by the National Congress, and the measures adopted during such states are expressly subject to constitutional review.

9.5.2 Legislation on Telecommunications and the Media

The Dominican legal framework for telecommunications is based primarily on the General Telecommunications Law (153-98), which establishes specific provisions regarding the provision of services and the management of the radio spectrum.²⁰³ This legislation created the Dominican Telecommunications Institute (Indotel) as the state regulatory body, endowed with functional, jurisdictional, and financial autonomy. Indotel has the authority to regulate the market, ensure universal service, manage the spectrum, and resolve disputes among service providers. Unlike a

²⁰³Dominican Republic. (May 27, 1998). *General Telecommunications Law (Law No. 153-98)*. Official Gazette No. 9,983. Art. 1.

purely technical approach, Indotel has also taken on roles in defining cybersecurity strategies and the national digital agenda.

Law No. 6132 on Freedom of Expression and Dissemination of Thought²⁰⁴, enacted in 1962, has specific implications for the practice of journalism in the country. Although this law prohibits prior censorship and establishes a framework of formal freedoms—which is consistent with constitutional provisions—it has been criticized for maintaining criminal penalties for so-called “speech crimes” (defamation and libel). However, the Constitutional Court has issued rulings overturning certain articles of this law that imposed prison sentences for defamation against public officials, thereby strengthening the protection of critical speech.²⁰⁵ This demonstrates that case law has adequately fulfilled its oversight role, ensuring that legal provisions do not contravene the constitutional order or overstep their bounds in such a way that rights and freedoms are affected.

In the area of digital security and the protection of online users, the Dominican Republic has Law No. 53-07 on High-Tech Crimes and Offenses.²⁰⁶ The primary purpose of this legislation is the comprehensive protection of information systems and the punishment of computer, cyber, and telecommunications crimes. The law defines and severely punishes conduct such as unauthorized access to systems, sabotage, data tampering, and the interception or spying on communications without prior authorization from a competent judge. To ensure its effective enforcement and prosecution, the law provided for the creation of specialized units, such as the Department for the Investigation of High-Tech Crimes and Offenses (DICAT) within the National Police, and the Division for the Investigation of Computer Crimes (DIDI), attached to the National Department of Investigations.

Another fundamental pillar of the regulatory framework is Law No. 172-13 on the Protection of Personal Data,²⁰⁷ which guarantees respect for individuals’ privacy and honor regarding the processing of their information in public and private files or databases. This law establishes procedural rules for the exercise of the *Habeas Data* remedy, granting citizens the inalienable right to access, correct, update, or delete their personal data in the event of error or inaccuracy. In addition, it establishes strict operational oversight of Credit Information Agencies (SIC) and strictly prohibits the collection of “sensitive data”—such as political opinions, religious beliefs, health status, or sexual preferences—without the free, express, and written consent of the data subject.

Finally, as mentioned earlier, Law 1-24 was recently enacted in the country, creating the National Intelligence Directorate (DNI). This law has been strongly criticized by various sectors of civil society and the press for containing provisions that, in their original wording, could compel the disclosure of private information without the need for a prior court order, potentially undermining the secrecy of communications and privacy protections.²⁰⁸

In addition to criminalizing cybercrimes, the Dominican Republic has developed public policies aimed at preventing and managing risks in cyberspace. The National Cybersecurity Strategy 2030²⁰⁹ establishes strategic objectives to protect critical national infrastructure, promote a national culture

²⁰⁴Dominican Republic. (December 15, 1962). *Law No. 6132 on the Expression and Dissemination of Thought*. Official Gazette No. 8,725.

²⁰⁵Constitutional Court of the Dominican Republic. (February 19, 2016). *Ruling TC/0075/16*. — Declared unconstitutional Articles 30, 31, 34, 37, 46, 47, and 48 of Law 6132, which provided for custodial sentences for defamation or libel against public officials and for the criminal liability of media outlets and journalists.

²⁰⁶Dominican Republic. (April 23, 2007). *Law No. 53-07 on High-Tech Crimes and Offenses*. Official Gazette No. 10,416.

²⁰⁷ Dominican Republic. (December 15, 2013). *Law No. 172-13, which aims to provide comprehensive protection for personal data contained in files, public records, databases, or other technical means of data processing intended for reporting purposes*. Official Gazette No. 10,737. <https://dgii.gov.do/transparencia/marcoLegal/Leyes/Ley172-13.pdf>

²⁰⁸Inter-American Press Association. (April 2024). *Dominican Republic Report to the Mid-Year Meeting*. <https://www.sipiapa.org/notas/1216584-republica-dominicana..>, <https://www.sipiapa.org/>.

²⁰⁹Dominican Republic. (June 14, 2022). *Decree No. 313-22 approving the National Cybersecurity Strategy 2030*. Official Gazette No. 11,069. <https://cnccs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf>

and education on cybersecurity, and develop the legal and institutional framework in this area. As part of this sectoral regulatory evolution, INDOTEL issued Resolution No. 126-2021, which establishes the Cybersecurity Regulations for the Provision of Internet Access Services.²¹⁰ This resolution imposes essential obligations on public service providers to safeguard the integrity of networks and protect users from digital vulnerabilities and threats.

At the same time, the country has promoted the modernization of its commercial and judicial infrastructures to adapt them to the digital ecosystem. Law No. 126-02 on Electronic Commerce, Documents, and Digital Signatures²¹¹ laid the early groundwork for granting legal validity and evidentiary weight to electronic transactions, democratizing access to global markets and revolutionizing the way Dominican society produces and safeguards information.

The Dominican government has begun to draft regulatory guidelines for the adoption of cutting-edge tools. Through Decree 498-23, the Executive Branch enacted the National Artificial Intelligence Strategy (ENIA),²¹² with the aim of democratizing the use of ICTs, increasing the competitiveness of the productive sector, and modernizing the government under the coordination of the Cabinet for Innovation and Digital Development.

9.5.3 Specific Regulation on Platforms and/or Content Regulation

Like other countries in the region, the Dominican Republic currently lacks a specific, enforceable law regulating digital social media platforms as internet intermediaries or establishing a limited liability regime similar to U.S. Section 230 or the European Digital Services Act (DSA).

In the tax sphere, the General Directorate of Internal Revenue (DGII) implemented General Rule 07-2023, which establishes the mechanism for collecting the Tax on the Transfer of Industrialized Goods and Services (ITBIS) on digital services provided from abroad (such as Netflix or Spotify), although this is purely a tax measure and does not involve regulation of the moderation of content offered by these platforms.²¹³

Given this sector-specific regulatory gap, control over discourse in the digital environment is de facto carried out through Law No. 53-07 on High-Tech Crimes and Offenses.²¹⁴ This legislation extends traditional criminal liabilities to cyberspace, directly criminalizing “content-related offenses.” For example, Articles 21 and 22 punish defamation and public slander committed through electronic, computer-based, or telematic means with prison terms and fines. It also severely punishes the dissemination of child pornography (Art. 24) and the illicit trade in goods and services over the internet (Art. 20). Although this law does not directly regulate technology companies as intermediaries, it does impose obligations on them to cooperate; for example, it requires service providers to retain users’ traffic and connection data for a minimum period of 90 days to facilitate criminal investigations (Art. 56).

²¹⁰Dominican Telecommunications Institute. (December 14, 2021). Resolution No. 126-2021 establishing the Cybersecurity Regulations for the Provision of Internet Access Services. <https://drive.google.com/open?id=1oXwB-XYxmBSEfKNMco27-BOxb6HaGe3g>

²¹¹Dominican Republic. (September 4, 2002). Law No. 126-02 on Electronic Commerce, Digital Documents, and Digital Signatures. Official Gazette No. 10,172. <https://indotel.gob.do/transparencia/marco-legal/ley-126-02/>

²¹²Dominican Republic. (October 11, 2023). Decree No. 498-23 declaring the adoption and application of Artificial Intelligence in the Dominican Republic to be of national interest and approving the National Artificial Intelligence Strategy (ENIA). Official Gazette No. 11,109. <https://ogtic.gob.do/wp-content/uploads/2023/10/Decreto-498-23.pdf>

²¹³General Directorate of Internal Revenue. (August 17, 2023). General Regulation No. 07-2023 on the Registration and Administration of Digital Service Providers. <https://dgii.gov.do/legislacion/normasGenerales/Documents/2023/Norma-07-23.pdf>

²¹⁴Dominican Republic. (April 23, 2007). Law No. 53-07 on High-Tech Crimes and Offenses. Official Gazette No. 10,416. <https://dgii.gov.do/transparencia/marcoLegal/Leyes/Ley53-07.pdf>

To address this shortfall and establish a modern governance framework, the country is currently debating the Draft Organic Law on Freedom of Expression and Audiovisual Media,²¹⁵ which devotes an entire chapter (Chapter IV) to the regulation of “Internet Content Platforms” and sets as a specific objective the guarantee of universal access to the internet. As of January 2026, this draft organic law had not received a favorable report from the Senate.

This proposal, applicable to social media platforms and commercial search engines whose user base exceeds 10% of the country’s internet users (excluding private messaging services that moderate content), requires that these companies’ community guidelines be consistent with international human rights standards. It introduces robust active transparency obligations, requiring platforms to publish their terms of service clearly in Spanish, to disclose how their recommendation algorithms work, and to provide detailed semiannual reports on any content restrictions or removals they implement.

The bill establishes due process safeguards for users in the face of algorithmic moderation. The initiative proposes that individuals affected by the suspension of their accounts or the removal of their posts be notified in advance, providing them with detailed reasons and a swift, accessible, and free appeal mechanism. Furthermore, in Article 24, it defines a regime of conditional civil liability for intermediaries (similar to the “safe harbor” model), establishing that platforms will only be liable for damages resulting from third-party posts if, after receiving a specific court order, they fail to take the necessary measures to disable such content (Art. 24). However, there are obvious gaps. There is no reference whatsoever to automated content moderation or artificial intelligence in general, and it lacks sufficiently developed regulations on micro-targeting or the use of *bots*, which will not be enough to strengthen the country’s electoral regulations. Nor does it include or promote media literacy initiatives among the population.²¹⁶

And although the legislative proposal seeks to modernize the law for the digital age, it also contains provisions regarding journalistic work, aiming to protect it from prior censorship. The proposal seeks to safeguard the practice of journalism through the absolute protection of professional secrecy and the inclusion of a conscience clause for journalists, but it has not been without criticism, amid concerns that it could also be used to criminalize journalistic work. A reading of Articles 16 through 18 reveals that it could criminalize the use of pseudonyms and may end up giving precedence to the right to honor of public figures even over society’s right to be properly informed, which could undermine journalistic work by exposing it to reprisals.

Another notable innovation is the creation of the National Institute of Communication (INACOM), a decentralized regulatory body with functional autonomy that would replace the former National Commission on Public Entertainment and Radio Broadcasting and would have the power to oversee accessibility and promote local culture. However, one of the main criticisms focuses on INACOM’s excessive concentration of technical and enforcement powers, as it is considered to lack adequate external checks and balances.²¹⁷

²¹⁵Dominican Republic. (2024). *Draft Organic Law on Freedom of Expression and Audiovisual Media*. Legal Advisory Office of the Executive Branch. <https://www.consultoria.gov.do/Documents/GetDocument?reference=a89391e1-c92d-4389-b673-81dd9e04ae69>

²¹⁶Chamber of Information and Communication Technologies (CAESCO). (May 6, 2025). *Preliminary Report on the Draft Organic Law on Freedom of Expression and Audiovisual Media of the Dominican Republic*. <https://caesco.org/wp-content/uploads/2025/05/Informe-preliminar-sobre-el-Proyecto-de-Ley-Libertad-de-Expresion.pdf>

²¹⁷Chamber of Information and Communication Technologies (CAESCO). (May 6, 2025). *Preliminary report on the draft Organic Law on Freedom of Expression and Audiovisual Media of the Dominican Republic*. <https://caesco.org/wp-content/uploads/2025/05/Informe-preliminar-sobre-el-Proyecto-de-Ley-Libertad-de-Expresion.pdf>

9.5.4 Data Protection and Privacy Legislation

The Dominican Republic has specific legislation in this area: Law No. 172-13 on the Protection of Personal Data.²¹⁸ The primary purpose of this legislation is the comprehensive protection of personal data contained in files, public records, or databases—whether publicly or privately owned—with the firm aim of guaranteeing the right to honor and privacy. The law operationalizes the constitutional remedy of *Habeas Data*, providing citizens with direct legal tools to ascertain the existence of their data and to demand the correction, updating, deletion, or blocking of information that is inaccurate, erroneous, discriminatory, or has been collected unlawfully.

The processing of information under this legal framework must be governed by a set of non-negotiable guiding principles, such as data quality, lawfulness, fairness, security, and purpose limitation; ensuring that the information collected is not used for purposes other than those that motivated its original collection. One of the pillars of the law is the requirement for the data subject's free, express, and informed consent to the processing and transfer of their data, except in very specific cases involving publicly available sources or national security purposes.

The law establishes a regime of enhanced protection for so-called “sensitive data”—data that reveals racial origin, political opinions, religious beliefs, union membership, as well as information regarding health and sex life—categorically prohibiting the creation of files that store such data without the explicit, written consent of the individual. The legislation also addresses the cross-border flow of information, permitting the international transfer of data only with the user's authorization or under strict legal conditions, such as judicial cooperation and the implementation of international treaties.

Despite the enshrinement of this broad range of rights, in practice, the design of Law 172-13 reflects an approach that is markedly skewed toward the regulation of the financial sector and credit histories. A large portion of its provisions is devoted to establishing the operating rules for Credit Information Companies (SICs) or credit bureaus. To ensure compliance in this specific sector, the law grants the Superintendency of Banks the authority to inspect, monitor, and impose administrative sanctions, thereby establishing this entity as the exclusive oversight body for databases intended to provide credit reports.

Perhaps because of this highly specialized approach, the Dominican Republic lacks an independent oversight authority with general jurisdiction over data protection—such as a National Data Protection Agency. Since administrative oversight for credit-related matters rests solely with the Superintendency of Banks, the protection of rights against abuses committed by digital platforms, social media, telecommunications companies, or mobile applications falls into an administrative vacuum.

Consequently, to defend themselves against the abusive collection, algorithmic profiling, or unauthorized commercialization of their information by big tech companies, ordinary citizens are forced to pursue their claims through *Habeas Data* proceedings in civil courts of first instance. This lack of a streamlined, preventive, and specialized institutional channel creates barriers to access to justice and may limit the Dominican State's ability to audit or impose sanctions *ex officio* on the mass processing of data in digital environments.

²¹⁸Dominican Republic Congress. (December 15, 2013). *Law No. 172-13, which aims to provide comprehensive protection for personal data contained in files, public records, databases, or other technical means of data processing used for reporting purposes*. Official Gazette No. 10,737. <https://dgii.gov.do/transparencia/marcoLegal/Leyes/Ley172-13.pdf>

9.5.5 Specific Regulations for the Protection of Vulnerable Groups

The protection of vulnerable groups in the Dominican digital ecosystem lacks a unified legal framework; rather, it is scattered across a patchwork of regulations that justice system operators must synthesize to address current challenges.

The governing law regarding children is Law No. 136-03, which establishes the Code for the System of Protection and Fundamental Rights of Children and Adolescents.²¹⁹ Article 26 of this law establishes the absolute right to protection of one's image and privacy, strictly prohibiting the dissemination of any data, information, or image that could affect the comprehensive development of minors or expose them to public ridicule. Although this provision is fully applicable to digital media and social media, its enforcement mechanism is designed for traditional media and lacks agile tools to require international platforms to immediately remove harmful content. Institutions such as the National Council for Children and Adolescents (CONANI) and the National Directorate for Children, Adolescents, and Families (DINNAF) play an active role in monitoring, although their ability to respond is limited by the speed at which content spreads in the digital environment.

With regard to gender-based violence, there is a significant gap between the current legal framework and the reality of the digital world. Law 24-97 on Domestic Violence,²²⁰ enacted before the rise of social media, does not criminalize digital violence. Faced with this gap, prosecutors and judges resort, on a supplementary basis, to Law 53-07 on High-Tech Crimes and Offenses²²¹ to prosecute serious conduct such as sexual blackmail, extortion, or the non-consensual dissemination of intimate images. However, this technical approach often obscures the gender-based aspect of the aggression, treating these acts as crimes against honor or generic computer offenses.

Another essential layer of protection for vulnerable groups comes from Law No. 172-13 on the Protection of Personal Data.²²² This law provides a crucial safeguard against digital discrimination by more rigorously defining and protecting "sensitive data." The law prohibits the processing, without express written consent, of information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as data concerning an individual's health or sex life. This provision is vital for protecting minorities and stigmatized groups from discriminatory profiling or undue exposure on digital platforms and in databases. However, as we have noted, the law has a specific focus on financial matters—an area where discrimination certainly can occur—but it also underscores once again that a law with a broader scope would be preferable.

Despite these legal tools, the Dominican government acknowledges that the current framework is insufficient to provide preventive and effective protection. The Ministry of Women²²³ has advocated for reforms, including a bill on violence against women.²²⁴ Initiatives such as the reform of the Penal

²¹⁹Dominican Republic. (August 7, 2003). *Law No. 136-03 establishing the Code for the System of Protection and Fundamental Rights of Children and Adolescents*. Official Gazette No. 10,234. https://www.poderjudicial.gob.do/wp-content/uploads/2021/01/Ley_136-03.pdf

²²⁰Dominican Republic. (January 27, 1997). *Law No. 24-97 amending the Penal Code, the Code of Criminal Procedure, and the Code for the Protection of Children and Adolescents*. Official Gazette No. 9,945. https://www.oas.org/dil/esp/Ley_24-97_Republica_Dominicana.pdf

²²¹Dominican Republic. (April 23, 2007). *Law No. 53-07 on High-Tech Crimes and Offenses*. Official Gazette No. 10,416. <https://dgii.gov.do/transparencia/marcoLegal/Leyes/Ley53-07.pdf>

²²²Congress of the Dominican Republic. (December 15, 2013). *Law No. 172-13, which aims to provide comprehensive protection for personal data stored in files, public records, databases, or other technical means of data processing intended for reporting purposes*. Official Gazette No. 10,737. <https://dgii.gov.do/transparencia/marcoLegal/Leyes/Ley172-13.pdf>

²²³Ministry of Women of the Dominican Republic. (2024). *Innovation in legislative proposals for the eradication of gender-based violence*. <https://mujer.gob.do/index.php/noticias/itemlist/tag/Ley%20Integral%20de%20Violencia>

²²⁴Ministry of Women of the Dominican Republic. (December 12, 2022). *Executive Branch Submits Drafts of the Comprehensive Law on Violence Against Women and the Reform of the Law on Human Trafficking and*

Code,²²⁵ which specifically criminalizes offenses such as cyberbullying and digital gender-based violence, have moved forward. Undoubtedly, these reforms represent significant progress in equipping the justice system with clear criminal offenses that recognize the severity of online attacks and establish expedited protection mechanisms for victims through a more robust and preventive framework. However, according to the Ministry of Women itself²²⁶ and international organizations, these reforms are still insufficient to adequately guarantee the rights of women and girls.²²⁷

9.5.6 Digital Electoral Regulation

The regulations governing democratic processes in the Dominican Republic are based on the Organic Law on the Electoral System (Law No. 20-23)²²⁸ and the Law on Political Parties, Groups, and Movements (Law No. 33-18).²²⁹ This legal framework grants the Central Electoral Board (JCE) the highest authority to organize and oversee elections, endowing it with the governing power to regulate campaign timelines, manage the use of the media, and guarantee constitutional principles such as fairness and transparency in the electoral process.

The emergence of social media as the primary arena for public debate has created tensions between electoral oversight and fundamental rights. The electoral authority is making administrative efforts to uphold the rules of the game. Through official proclamations, the JCE urges political organizations and citizens to observe the silence period, or “electoral blackout,” across all media platforms, expressly extending this call to the digital sphere. The enforcement of these measures in the globalized cyberspace is extremely complex at the operational level.

Furthermore, Law 33-18 originally sought to establish strict control over the internet by criminalizing the dissemination of “fake news” or “negative messages” against candidates. However, through Ruling TC/0092/19²³⁰, the Constitutional Court struck down those provisions for violating freedom of expression, ruling that political criticism on social media enjoys enhanced protection and prohibiting the State from acting as a censor of speech under electoral pretexts. This is further proof that the Dominican constitutional system has functioned effectively where legislation has overstepped its bounds.

Finally, the greatest challenge currently facing the Dominican electoral system lies in regulating political financing in the online environment. In online environments, political propaganda has shifted toward hyper-personalized and micro-segmented digital advertising. While political parties are required to report campaign expenditures, the JCE’s technical capacity was designed to audit traditional media and remains limited in its ability to monitor digital advertising in real time. This

Smuggling. <https://mujer.gob.do/index.php/noticias/item/1055-poder-ejecutivo-deposita-proyectos-de-ley-integral-de-violencia-contras-las-mujeres-y-reforma-de-ley-de-trafico-y-trata-de-personas>

²²⁵Dominican Republic. (August 15, 2025). *Law No. 74-25 establishing the Penal Code of the Dominican Republic*. Official Gazette No. 11,124. <https://revistamercado.do/wp-content/uploads/2025/08/Ley-Nu%CC%81m.-74-25-Co%CC%81digo-Penal-RD.pdf>

²²⁶Ministry of Women of the Dominican Republic. (July 11, 2024). *Ministry of Women reiterates that the reform of the Penal Code violates women’s human rights*. <https://mujer.gob.do/index.php/noticias/item/1397-ministerio-de-la-mujer-reitera-reforma-del-codigo-penal-vulnera-los-derechos-humanos-de-las-mujeres>

²²⁷Amnesty International. (August 14, 2025). *Dominican Republic: New Penal Code Fails to Guarantee the Rights of Women and Girls*. <https://www.amnesty.org/es/latest/news/2025/08/republica-dominicana-nuevo-codigo-penal-no-garantiza-los-derechos-de-las-mujeres-y-ninas/>

²²⁸Dominican Republic. (February 17, 2023). *Law No. 20-23 on the Electoral System*. Official Gazette No. 11,092. <https://jce.gob.do/DesktopModules/Bring2mind/DMX/API/Entries/Download?EntryId=31481>

²²⁹Dominican Republic. (August 13, 2018). *Law No. 33-18 on Political Parties, Groups, and Movements*. Official Gazette No. 10,917.

<https://jce.gob.do/DesktopModules/Bring2mind/DMX/API/Entries/Download?EntryId=23405>

²³⁰Constitutional Court of the Dominican Republic. (May 21, 2019). *Ruling TC/0092/19. Direct action for unconstitutionality against Article 44, paragraph 6, of Law No. 33-18 on Political Parties, Groups, and Movements*. <https://tribunalsg.gob.do/mantenimiento/sentencias/TC-0092-19.pdf>

asymmetry makes it very difficult to trace the origin of funds and control the proliferation of covert online campaigns.

9.6 Alignment with UNESCO Guidelines: Dominican Republic

An analysis of the Dominican Republic's regulatory and institutional framework, in light of the UNESCO Guidelines for the Governance of Digital Platforms, reveals a scenario of contrasts: a constitutional framework that guarantees rights coexists with sector-specific regulatory gaps and practical challenges in the digital ecosystem.

At its core, the country demonstrates strong conceptual alignment with international human rights standards. The Constitution not only prohibits prior censorship and enshrines the right of reply but also grants constitutional status to data protection through the concept of *habeas data* and elevates international treaties to the level of constitutional law. This robust framework has enabled the Constitutional Court to act as an effective check; evidenced by the aforementioned ruling TC/0092/19, which dismantled legislative attempts to criminalize “fake news” or “negative messages” during election campaigns, setting the precedent that political criticism on social media enjoys enhanced protection against the State's temptations to censor.

However, with regard to the specific regulation of internet intermediaries, the country currently lacks a systemic governance model. In the absence of a “safe harbor”-type limited liability regime, control over online speech *de facto* falls under Law No. 53-07 on High-Tech Crimes and Offenses. Relying on criminal law to address “content-based offenses” (such as electronic defamation) poses risks of disproportion and asymmetry in relation to UNESCO guidelines, which promote a civil and preventive approach rather than a punitive one.

In an effort to address this shortfall, the Dominican government has submitted for debate a Draft Organic Law on Freedom of Expression and Audiovisual Media, which incorporates requirements aligned with UNESCO's guidelines. The proposal requires major platforms to align their community guidelines with human rights standards, make recommendation algorithms transparent, issue semiannual moderation reports, and establish fast and free appeal channels, while also instituting a system of conditional liability.

However, the bill contains critical omissions and risks: it fails to address automated moderation, artificial intelligence, *bot* armies, or microsegmentation—elements essential for protecting electoral integrity in an environment where the authority (the JCE) already acknowledges technical limitations in auditing digital advertising. Furthermore, the bill's intention to criminalize the use of pseudonyms directly conflicts with the protection of online anonymity—a pillar internationally upheld to safeguard critical and dissenting voices—and stands in direct tension with the Guidelines' aim to propose a robust regulatory framework for human rights. In any case, as of January 2026, the bill had not yet received a favorable report from the National Senate, so its legislative process has not moved forward.

Finally, the institutional framework and the protection of vulnerable populations reveal a fragmentation that hinders the application of due diligence. Although laws such as the Personal Data Protection Act (Law 172-13) safeguard the processing of “sensitive data” (such as sexual orientation or political affiliation), the absence of an independent National Data Protection Authority forces citizens to pursue legal action against any abuses committed by big tech companies, creating enormous barriers to access to justice.

Similarly, the protection of children and women against cyberbullying and digital violence lacks agile mechanisms to demand the immediate removal of harmful content from platforms, forcing judicial authorities to rely on analog laws or generic cybercrime provisions that ultimately downplay the severity of these attacks. This fragmentation, coupled with the proposal to concentrate enforcement powers in a potential new National Institute of Communication (INACOM), as outlined in the

aforementioned Organic Law on Freedom of Expression and Audiovisual Media without clear checks and balances, underscores the Dominican Republic's challenge of transitioning toward a digital ecosystem that not only connects its population but also structurally protects it through an approach that incorporates all relevant *stakeholders*.

10. Alignment with UNESCO Guidelines from a Regional Perspective

A cross-sectional analysis of the regulatory and institutional frameworks in Costa Rica, Guatemala, Honduras, El Salvador, Panama, the Dominican Republic, and Mexico reveals stark contrasts. Although all these countries share a robust constitutional framework that prohibits prior censorship and protects freedom of expression through a technology-neutral approach, the effectiveness of these guarantees is undermined by significant regulatory gaps. Thus, while the constitutions are aligned with the requirements of international law, in practice there are clear challenges and barriers.

UNESCO guidelines emphasize that digital governance must be grounded in a multi-stakeholder ecosystem, safeguarding human rights and requiring platforms to exercise strict due diligence. However, the region operates primarily under sector-specific approaches, with evident fragmentation in the regulatory framework. All too often, these approaches are reactive and punitive, still focusing on citizens' online behavior rather than on the system as a whole. This deviates from the model of shared responsibility, proactive transparency, and citizen empowerment required by international standards.

Regarding freedom of expression and the protection of civic space, the UNESCO Guidelines recommend that any restrictions imposed by states must pass a rigorous test of legality, legitimate purpose, necessity, and proportionality. While courts in Costa Rica and Mexico formally apply this test in their case law, the operational reality in the region is restrictive—at times severely so.

In El Salvador, the extension of the State of Emergency has legalized unrestricted state surveillance that encourages self-censorship and silences public debate. In Honduras and Panama, the retention of defamation and slander as criminal offenses facilitates judicial harassment of journalists through strategic lawsuits (SLAPPs), directly contravening the international call to decriminalize speech. This stifling of civic space is exacerbated by the documented use of surveillance technologies against the press and human rights defenders in several countries in the region, undermining the secure environment essential for the free flow of information.

Regarding platform governance, the UNESCO Guidelines establish the need for legal frameworks that grant conditional liability to intermediaries (such as safe harbor schemes) in exchange for non-negotiable statutory obligations regarding transparency, due process for users, and periodic human rights impact assessments. There are few examples of such legal frameworks in the region: Costa Rica took a historic step in April 2026 by passing the Law on the Governance of Digital Services and Electronic Commerce—the first comprehensive legislation of its kind in Central America—although even this progress falls short of the Guidelines' most stringent standards.

Guatemala, Honduras, El Salvador, and the Dominican Republic still lack modern laws defining the role of digital platforms and frameworks that require this type of conditional liability—or, if you will, that guarantee conditional immunity. Faced with this gap, governments resort to consumer protection laws or criminal codes, which discourage platforms from implementing appeal mechanisms that guarantee due process for citizens in the protection of their rights and freedoms in the face of content moderation decisions.

Although Costa Rica, Panama, and Mexico have made progress in incorporating provisions for conditional liability or “safe harbor”—through different avenues and with varying scopes—no country in the region has succeeded in imposing cross-cutting mandates that require big tech companies to ensure transparency in the operation of their algorithms or to guarantee that automated content moderation is sensitive to linguistic diversity and local cultural context, as emphatically demanded by UNESCO.

One of the most acute divergences from the UNESCO model lies in institutional design and the requirement for full regulatory autonomy. The Guidelines call for agencies responsible for regulating the digital ecosystem to be strictly independent from political and governmental control. However, in most of these countries, the relevant authorities often report directly to the executive branch. In Mexico, even though there have been significant legislative changes containing elements that are more in line with the Guidelines, the reality is that recent structural reforms have reduced or eliminated the constitutional autonomy of key regulators in the areas of telecommunications and government transparency, concentrating power in the central administration and dismantling the basic institutional checks and balances designed to prevent arbitrary state intervention.

The power imbalance in the face of corporate data extraction is exacerbated by shortcomings in privacy and digital literacy—elements that UNESCO considers enablers of citizen empowerment. With the exception of Panama and Mexico, which have comprehensive laws applicable to the private sector, the rest of the countries rely on the constitutional concept of *Habeas Data*, regulations exclusive to the public sector, or laws disproportionately focused on specific areas (such as credit histories in the case of the Dominican Republic).

Additionally, tolerated commercial practices such as *zero-rating* in countries like Honduras and El Salvador undermine net neutrality, trapping users in social media bubbles that limit access to the open internet. This technical limitation can fuel the spread of disinformation, which directly contradicts UNESCO's recommendation to provide populations with robust national policies on Media and Information Literacy to foster critical thinking, as well as the requirement under international human rights instruments and national constitutions to actively work toward guaranteeing the right to freedom of expression and, in particular, access to information.

Finally, in the area of democratic integrity, the UNESCO Guidelines urge States and platforms to conduct systemic human rights risk assessments, but none of the countries has framework legislation—or even national or regional guidelines—that would enable them to do so.

This is also particularly relevant in terms of mitigating risks that could affect electoral integrity. The tools available to protect electoral processes from algorithmic manipulation do not appear to be sufficient in the countries of the region, given that the current environment is more complex than ever before.

The shift of political propaganda to the digital sphere has outpaced the legal capacity of nearly all authorities in the region. Panama stands out as a regulatory pioneer by updating its Electoral Code to require transparency in the financing of digital advertising, prohibit the use of inauthentic accounts, and criminalize the malicious use of artificial intelligence. In contrast, in Costa Rica, Guatemala, and Mexico, electoral authorities have had to operate through voluntary agreements or precautionary measures lacking long-term enforcement power.

The most paradoxical omissions lie with El Salvador, which successfully implemented remote electronic voting but maintains a complete legal vacuum when it comes to regulating digital propaganda, and the Dominican Republic, whose authorities acknowledge their technical inability to audit foreign advertising microsegmentation, leaving the region's electoral processes exposed to the power of technology corporations and to the specific risks that have emerged following the digitization of electoral processes—risks that are now beginning to include particular threats stemming from the use of generative AI, in addition to those already identified in relation to algorithmic mediation on digital platforms.

A joint analysis of the seven countries studied shows that the region is at a critical regulatory and democratic crossroads. While the region's solid constitutional foundation represents an undeniable strength, the slow pace of translating these principles into modern, coherent legal frameworks leaves the digital ecosystem subject to fragmented, asymmetrical, and—all too often—reactive, if not punitive, governance.

To achieve true alignment with UNESCO's vision for a trustworthy internet as outlined in its Guidelines, it is imperative that states move beyond the temptation of government surveillance and a punitive approach centered on monitoring users, evolving toward a model of systemic shared responsibility anchored in coordinated regional cooperation and in which local and regional contexts are fully taken into account.

This requires an unavoidable commitment to establish truly independent regulatory authorities, close gaps in electoral oversight, and compel transnational technology platforms to practice active transparency, conduct impact assessments, and apply human rights due diligence. Only through comprehensive governance grounded in multi-stakeholder dialogue will it be possible to protect civic space online, mitigate systemic risks—including those posed by new developments in artificial intelligence—and ensure that the internet functions as an equitable enabler of freedoms and human rights, rather than as a barrier, to the region's democratic development.

11. Training workshops for Mexico, Central America, and the Caribbean

With the support of UNESCO and funding from the European Union, the I4T Global Knowledge Network organized a series of training workshops on the regulation of digital platforms in the context of the UNESCO Guidelines in Santo Domingo, Dominican Republic, in a hybrid format (in-person and online). This event was part of the UNESCO project titled “Safeguarding Freedom of Expression and Access to Information through the Implementation of the UNESCO Guidelines for the Governance of Digital Platforms,” which, like this report, is funded and supported by the European Union. The main objective of these sessions was to create a space for analysis and training on the implementation of the UNESCO Guidelines, promoting a human rights-based approach to regulating the digital ecosystem in the region.

To ensure a free and open environment for debate, the sessions were conducted under the *Chatham House Rule*, allowing attendees to use the information shared without revealing the identity or affiliation of the speakers. The event was organized through a broad inter-institutional and academic partnership. Among the organizing and collaborating entities were higher education institutions and global networks, such as the UPF Barcelona School of Management, which led the organization and delivery of the workshops; the Complutense University of Madrid; the Catholic University of Santo Domingo (UCSD), which served as the local organizer; the Global Network for Electoral Justice; and the Institute for Training and Studies in Democracy (IFED) of Costa Rica’s Supreme Electoral Tribunal.

The event brought together key actors in governance and the protection of rights in the digital sphere, incorporating a *multistakeholder* perspective. On the governmental and electoral side, several authorities from the region participated, including the Supreme Electoral Tribunal of Costa Rica, El Salvador’s Superior Electoral Tribunal, Honduras’ Electoral Court of Justice, Panama’s Electoral Tribunal, Mexico’s National Electoral Institute, and the Dominican Republic’s Superior Electoral Tribunal, as well as Panama’s National Public Services Authority, the Dominican Telecommunications Institute (INDTOEL), and the Dominican Republic’s Ministry of Technology and Innovation. From a citizen’s perspective, the event featured strong representation from civil society organizations, such as ARTICLE 19 (Mexico and Central America), Derechos Digitales and the Center for Digital Law Research (Costa Rica), SocialTIC and Cultivando Género (Mexico), the National Association of Corporate Lawyers (ANADE, also from Mexico), ACI Participa (Honduras), Dominicanos por Derecho (Dominican Republic), the Chamber of Information and Communication Technologies (CAESCO, also from the Dominican Republic), and the Pan American Institute of Law and Technology in partnership with the Internet Society (Panama).

11.1 Key Contributions and Conclusions of the Workshops

The first day of the workshops, held on December 8, 2025, focused on the central theme of “Regulation of Digital Platforms in the Public Interest.” The day began with an introductory session led by UNESCO, which served to present the objectives and priorities of the UNESCO Guidelines. It was emphasized that the goal is never to censor specific content, but rather to regulate the systems, processes, and algorithms of technology companies through a human rights-based approach and shared responsibility. This established the roadmap and general context that would guide the discussions over the next two days.

This was followed by the first session, which focused on the presentation of the report on the **“Mapping of the Regulatory Framework in Central America and the Caribbean”** mentioned

above. During this session, the most relevant findings of the regional assessment were presented, and the extent to which the countries in the region's regulations align with the UNESCO Guidelines was discussed. This technical presentation served as a starting point for a fruitful exchange of views with the authorities and civil society representatives in attendance, allowing them to discuss their institutional perspectives and set priorities at both the national and regional levels.

The presentation of the regional assessment sparked an initial exchange in which representatives from government agencies, academia, and civil society agreed that there is clear regulatory fragmentation. A profound paradox in the region was highlighted: while states have demonstrated high effectiveness in applying and collecting taxes (such as VAT) on cross-border digital services and *streaming* platforms, there is an almost total vacuum when it comes to requiring them to protect human rights or ensure transparency—an assessment shared by both civil society and government authorities.

The second session was dedicated to analyzing **“Regulatory Gaps and Coordinating Responses from Civil Society.”** The discussion delved into the regulatory gaps found in the region, placing special emphasis on the risks to the protection of human rights. It was a space for active listening where civil society organizations—participating both in person and online—were invited to present their main challenges, expectations, and concerns regarding attempts to regulate platforms and government intervention in their respective countries.

Voices from civil society and academia warned that the region is full of good proposals and documents, but that in practice they end up being “dead letters” due to a lack of political will. A representative from an electoral authority acknowledged this reality, highlighting that at the political level it has been very difficult to build consensus on regulating the digital environment, as political parties and candidates often benefit from manipulation and disinformation campaigns. The Dominican Republic itself was cited as an example, where electoral legislation does not address digital campaigns, yet legislative efforts to address them have failed to gain traction.

The representatives of the authorities present also expressed deep frustration regarding their efforts to engage with the platforms and collaborate. A representative of an electoral authority stated that these corporations “play in the big leagues” and always prioritize monetizing hate speech and polarization, and that they often have more technical and material resources than the authorities themselves. Civil society groups reported that platforms often ignore their reports of digital violence, state surveillance, or coordinated harassment, hiding behind internal policies or even the “social relevance” of problematic users. Furthermore, they criticized tech companies for frequently meeting with governments behind closed doors while excluding civil society from the dialogue.

A civil society representative highlighted the digital divide and stated that it is impossible to build effective digital governance if citizens and public servants lack basic media literacy, and as long as high dependence on and a lack of technological autonomy persist in the region.

Finally, various organizations pointed out that, in cases of digital violence, the state does not know how to respond, and victims lack clear channels for reporting incidents, often being shuffled from cybercrime units to prosecutors' offices and telecommunications agencies without finding an adequate solution—a situation that exacerbates citizens' vulnerability. This confirms the regional assessment that highlights regulatory gaps, fragmentation, and unclear jurisdictional boundaries among the relevant authorities.

The third and final session of the day took a purely practical approach, with the remainder of the session dedicated to the **“Periodic Table of the I4T Global Knowledge Network,”** which used this tool to facilitate a co-creation process, integrating real-world examples drawn from the regional report so that authorities and civil society organizations could work together on proposals to address these issues. The goal of this exercise was to design governance maps that would address specific regulatory needs without compromising guarantees of freedom of expression and other rights.

Divided into groups to work collaboratively, government officials and civil society representatives presented proposals for governance maps to address specific problems, generating several recommendations:

- **Hybrid moderation with local context:** One group emphasized that purely automated moderation using algorithms is ineffective and even dangerous in the region, since artificial intelligence is incapable of understanding subtleties, idioms, and cultural contexts, noting that even words with the same spelling can vary drastically in meaning from one country to another. Therefore, they presented a model that requires platforms to implement hybrid content moderation mechanisms, which use automation but include strict human oversight by moderators familiar with the local context, stressing that people must always make the final decisions. To this end, they also highlighted the importance of having robust appeal mechanisms and due process procedures that allow for the review of decisions and provide appropriate remedies when necessary.
- **Data Sovereignty:** A second group warned about the vulnerability of privacy and personal data at the regional level, noting that only 20% of the data centers storing Latin American information are located within the continent. They discussed the need to strengthen the protection of personal data and design regulatory mechanisms that empower citizens to demand the deletion of their information after a certain period of time, and that authorize authorities to protect particularly sensitive information (such as voter registries). To this end, it was noted that, in addition to strengthened regulations, it was necessary to create mechanisms for inter-institutional coordination.
- **Accountability Mechanisms/“Follow the Money”:** Finally, a third group analyzed possible alternatives for bringing foreign platforms under local jurisdiction when they have no physical presence in the countries of the region. The proposal suggested that, beyond electoral and telecommunications agencies, financial system supervisory authorities and banking and tax authorities can be key actors. Given that platforms rely on subscriptions, credit card payments, and locally monetized advertising, these types of authorities possess coercive power that they can use to, at the very least, ensure that the platforms come to the negotiating table. It was also emphasized that these types of authorities can play an important role in monitoring and moderating fraudulent online content, particularly when it relates to financial products, investments, and other banking transactions. The example also served to demonstrate that, in platform governance, it is necessary to think outside the box and assess the role that authorities and regulatory bodies—whose mandates differ from those typically considered when designing governance and regulatory frameworks for digital platforms—can play.

Finally, the first day concluded with a closing session that summarized the findings of the discussions and featured a collective reflection to define the essential regulatory priorities for the region over the next three to five years. This collective reflection yielded a clear mandate: in the face of transnational corporations that are beyond the reach of small countries acting in isolation, the top priority for regulators over the next three to five years must be to forge a stronger bloc of regional alliances that enables inter-institutional and supranational cooperation and coordination. It was also emphasized that a social pact is needed to unite states, relevant authorities, academia, and civil society in Central America and the Caribbean, enabling them to exert geopolitical pressure to demand respect for human rights, algorithmic transparency, and the ethical use of technology in the digital ecosystem.

The second day of the workshops, December 9, 2025, was organized around the theme “**Protecting Democracy in the Digital Age.**” The day began with the first technical session, titled “**Regulatory and Jurisprudential Responses to Electoral Disinformation.**” During this session, the main findings of the regional report on legislation aimed at combating disinformation and protecting the integrity of elections were presented, highlighting key lessons derived from case law. This presentation opened an important space for dialogue in which the region’s electoral authorities shared firsthand their experiences, operational challenges, and main concerns regarding online manipulation campaigns.

This was followed by an exchange of experiences between authorities and civil society. An electoral representative raised the dilemma of “when to respond to electoral disinformation without inadvertently giving it more visibility,” to which a representative from Panama responded with an example. The Panamanian official described how a digital monitoring center was created to focus on rapid fact-checking and, crucially, on providing advance civic education so that voters can learn to identify disinformation on their own. During this listening session, it was noted that the most common disinformation narrative in the region is one that seeks to erode the credibility of the electoral bodies themselves, often through unfounded accusations of fraud or by exploiting a lack of understanding of the processes. Consequently, it was concluded that efforts must be combined not only to protect the integrity of the processes but also to defend the institutional framework of the authorities and better explain their role as guarantors of free and fair electoral processes.

The program continued with a session titled “**Anatomy of Electoral Integrity in Latin America: From Disinformation to the Challenge of AI,**” which offered an in-depth analysis of recent electoral processes in various countries across the continent. The presentation not only highlighted success stories in institutional responses but also placed strong emphasis on the disruption posed by generative artificial intelligence and the emerging challenges this technology presents for propaganda and modern political campaigns.

During this session, a representative from the Costa Rican electoral authority noted that the main challenge for electoral bodies is how to respond to disinformation without the electoral authority becoming just another political actor. The shared conclusion was that authorities should prioritize intervening only when disinformation undermines the integrity of the electoral process (for example, by discouraging voting or committing gender-based violence to exclude candidates), and avoid becoming arbiters of intra-party falsehoods—for which, moreover, they lack the resources and objective tools.

The next session adopted a highly interactive approach, focusing on “**The Electoral Cycle and Digital Risks.**” Using UNESCO’s guide “*Elections in the Digital Age*” as a basis, authorities and civil society representatives worked together to identify threats to electoral integrity and human rights throughout the three critical stages of the democratic process: the pre-election period, election day, and the post-election phase.

Participants used the UNESCO guide to identify risks during the three defined stages of the electoral process. The discussion addressed the urgent need to regulate the use of Artificial Intelligence, highlighting how this technology lowers the cost and automates the creation of psychographic profiles and the distribution of false content, enabling the personalization of political persuasion to unprecedented levels. Civil society called for a focus on measures—such as those currently in place in the European Union—that prohibit political microsegmentation based on sensitive data.

This collaborative exercise laid the groundwork for the fourth and final practical session of the day, which aimed to chart a path “**Toward regional protocols to respect rights, preserve electoral integrity, and combat disinformation.**” Through this exercise, representatives from various sectors engaged in discussions at working groups to agree on priorities and outline joint solutions that safeguard democracy while scrupulously respecting human rights. It was agreed that, to effectively address threats to electoral processes, the response cannot depend solely on electoral bodies, which—often lack the visibility and budget necessary to combat hybrid campaigns. There was consensus that it is necessary to demand transparency in the financing of digital campaigns and to promote partnerships with universities and fact-checkers.

Finally, the second day concluded with a closing session that summarized the main conclusions from both days. Participants engaged in a collective reflection to define the roadmap and regulatory priorities needed to protect democracy in the region in the coming years. It was agreed that strengthening the technical capacities of states, adapting regulatory frameworks to the technological reality, and promoting digital literacy are key to safeguarding public trust in the region’s democratic systems. The main priority identified following the first day’s sessions was also reiterated: in the

coming years, regulators must prioritize the creation of strong regional alliances. Furthermore, Central America and the Caribbean need a multisectoral social pact to exert geopolitical pressure and guarantee human rights, algorithmic transparency, and ethics in the digital environment.

11.2 Analysis of Key Regional Challenges and Priorities

The workshops described above also served to foster dialogue and gather direct feedback from participants on the UNESCO Guidelines, as well as to obtain input that will help define the support and evidence that the I4T Global Knowledge Network can provide to assist in building effective governance frameworks in the Central American and Caribbean regions. This input was gathered from both government officials and representatives of civil society organizations.

A series of questions and topics were posed to government and civil society representatives from Mexico, Honduras, El Salvador, Panama, Costa Rica, and the Dominican Republic who attended the workshops.

Based on this exercise, discussions centered on the following thematic areas to validate the workshops' main conclusions:

- **A paradigm shift toward process-based regulation:** There was consensus that regulation should not focus on individual pieces of content—to mitigate the risk of censorship—but rather on the systems and processes of the platforms. The need to demand transparency in content moderation and recommendation policies, the functioning of algorithmic systems, advertising practices, and user reporting mechanisms was emphasized.
- **Regulatory convergence and shared responsibility:** A disconnect was evident between regulators and legislators in addressing the phenomenon of disinformation. In light of this, it was argued that digital challenges are global and transcend national borders. A public-private diplomacy strategy was proposed, aimed at creating regional blocs that would provide greater bargaining power vis-à-vis large technology companies, thereby mitigating the lack of local representation in smaller countries.
- **Governance Based on Existing Institutional Infrastructure:** Rather than creating new bureaucracies or immediately amending current legislation, it was recommended to leverage the experience and technical capabilities of already established agencies (such as electoral authorities, telecommunications regulators, and banking supervisory agencies, a proposal that emerged from the workshops themselves), by fostering mechanisms for inter-institutional coordination. However, emphasis was also placed on the need to continue working on capacity-building for these institutions and on establishing international support frameworks for these purposes, as well as for sharing experiences and evidence regarding regulatory and governance mechanisms that have proven effective.

Questions were also raised regarding the specific challenges identified for Central America and the Caribbean:

- **Electoral vulnerability and lack of technological autonomy:** It was noted that platforms operate as information battlefields during electoral processes, while national legal frameworks are often insufficient to regulate “dark money” in advertising and digital campaigns. Added to this is a high dependence on foreign infrastructure (cloud servers and artificial intelligence services), which compromises digital sovereignty and the protection of personal data in the region.
- **Digital Literacy and Sociocultural Context:** It was noted that simply providing internet access is insufficient without fostering citizens' critical thinking skills to identify disinformation

and hate speech. Furthermore, criticism was directed at platforms' application of uniform moderation policies, which often ignore cultural nuances and indigenous languages in each country, resulting in ineffective or discriminatory actions.

- **The Challenge of Generative Artificial Intelligence:** Generative AI was identified as a new systemic risk. The urgency of establishing clear ethical and regulatory frameworks to prevent abuses—such as the proliferation of *deepfakes*—that could violate human dignity or undermine the integrity of democratic processes was emphasized.

The I4T Global Knowledge Network also raised a series of questions on which information was sought during the workshops themselves and through direct conversations. The following was compiled from transcripts of the general workshop discussions and other specific conversations, as well as from previously established points and objectives:

- **Impact of the UNESCO Guidelines on the region's regulatory frameworks.** In assessing the impact of the I4T Guidelines in the region, no direct evidence was found that they have inspired concrete regulatory improvements to date; however, participants described them as a valuable “compass” for the region. In contrast, European frameworks, such as the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR), have indeed served as inspiration and were frequently cited as the standards to follow. As we have seen, however, although there is much work to be done in the region, several examples of alignment have been found in the existing legislation, the main one being the constitutional frameworks of the various countries.
- **Perceptions and Implementation Challenges.** It is important to note that the I4T Guidelines are not rejected by local stakeholders. The real obstacle lies in the challenge of “regional adaptation.” The main concern of stakeholders is not the guidelines themselves, but the practical difficulty of applying them in small markets. In these countries, giant technology companies generally do not have physical offices or legal representatives, making it nearly impossible to hold them accountable at the local level.
- **Areas of Opportunity and Identified Gaps.** During the sessions and discussions, several gaps were highlighted that require ongoing attention from UNESCO:
 - **Linguistic and Cultural Nuances:** It became evident that the guidelines need to take a much deeper approach to indigenous languages and local dialects, contexts in which content moderation by platforms is often nonexistent.
 - **Agility in the Face of Artificial Intelligence:** There is a latent concern that the speed at which generative AI is evolving is rapidly outpacing the responsiveness of current regulatory frameworks.
 - **Influence of small states:** An urgent need was identified to create specific protocols for those countries that, due to their size, lack the individual negotiating power necessary to confront large platforms.
- **Expectations for UN Agencies:** Faced with these challenges, stakeholders have very clear expectations regarding the support they require from United Nations agencies. First, they request support in regional diplomacy to help small nations form strong blocs that will enable them to negotiate collectively with Big Tech. Second, they require technical assistance to develop specialized monitoring units and digital forensic tracking capabilities. Finally, they expect the UN to facilitate effective spaces for dialogue, promoting a multi-stakeholder model that brings together government, academia, and civil society around the same table.

Table 10. Summary of Findings

Specific Issue	Workshop Findings
Have the I4T Guidelines inspired better regulation?	There is no direct evidence. The guidelines were described as a compass for the region.
Have other global frameworks inspired better regulation?	Yes. The European Union’s Digital Services Act (DSA) and the General Data Protection Regulation (GDPR) were frequently cited as standards.
Are the I4T Guidelines rejected? Why?	No, they are not rejected. However, there is a challenge of “regional adaptation.” The main concern is not the guidelines themselves, but the difficulty of applying them to small markets where <i>Big Tech</i> companies do not have physical offices or legal representatives who can be held accountable.
Have any gaps been identified by the UNESCO team?	Yes. Several gaps for continuous improvement were identified: 1. Linguistic and Cultural Nuances: The guidelines need to place greater emphasis on indigenous languages and local dialects, where moderation is often nonexistent. 2. Agility vs. AI: The pace of evolution of generative AI is outpacing current frameworks. 3. Influence of Small States: The need for specific protocols for countries that lack individual bargaining power with the platforms.
What Do Stakeholders Expect from UN Agencies?	Stakeholders are seeking: 1. Support for Regional Diplomacy: To help small nations form blocs to negotiate with big tech companies. 2. Technical Assistance: Providing expertise for specialized monitoring units and digital forensic tracking. 3. Effective Forums for Dialogue: Facilitating a “ <i>multi-stakeholder</i> ” model where government, academia, and civil society can come together to collaborate and engage with the platforms.

Source: Prepared by authors.

All the information and opinions gathered enable the I4T Global Knowledge Network to identify a list of key points to advance from Central America and the Caribbean, which can help the network focus its collaboration with the region in the coming years:

- **Linguistic Sovereignty:** Work to ensure that platforms provide transparency reports specifically for indigenous and regional languages, not just for “Spanish” as a whole. The differences in how Spanish is spoken across the region’s countries must also be taken into account.
- **Regional Negotiation Protocols:** Develop a framework for small states to negotiate as a bloc with the platforms and to coordinate regulatory and governance actions, ensuring that they are not overlooked due to the size of their markets.

- **Rapid-Response Forensic Analysis:** UNESCO could facilitate a “Global Technical Assistance Center” (Helpdesk) or a network of experts that electoral authorities in small states can turn to during active election cycles to verify disinformation generated by artificial intelligence.
- **Further explore the role of banking authorities in supervising platforms and existing risks:** Explore the adoption of a “Banking Supervision” model for platform governance. This approach leverages the high institutional autonomy and technical expertise of financial regulators to manage platforms as “systemic risks,” using proven “Know Your Customer” (KYC) protocols to trace funding (disinformation and advertising interference) and explore mechanisms to freeze payments to platforms.

Discussions in Central America and the Caribbean reveal a consensus on the need for a regulatory paradigm shift: moving from restrictive content moderation toward transparent oversight of digital platforms’ systems, processes, and algorithms. While UNESCO’s I4T Guidelines are valued as a guiding compass, operational reality shows that small nations lack the individual influence to hold *Big Tech* accountable. This vulnerability is exacerbated by systemic threats such as electoral disinformation, the emergence of Generative Artificial Intelligence, and the implementation of global policies that systematically ignore indigenous languages and local cultural nuances.

To address these structural challenges, the I4T Knowledge Network must focus its collaboration on empowering the region through collective action and institutional innovation. Strategic priorities include establishing protocols to enable countries to negotiate as a unified regional bloc, demanding linguistic sovereignty in transparency reports, and deploying specialized technical assistance. Furthermore, it is essential to leverage existing government infrastructure by exploring innovative models—such as involving banking authorities to conduct financial oversight of platforms—in order to identify and address systemic risks.

12. Conclusions and Recommended Actions

12.1 Key Findings

A cross-sectional analysis of the regulatory and institutional frameworks of Costa Rica, Guatemala, Honduras, El Salvador, Panama, the Dominican Republic, and Mexico—compared with the UNESCO Guidelines and informed by the *multistakeholder* dialogues held during the regional workshops—allows us to draw the following structural conclusions:

1. Discrepancy between constitutional protections and operational reality. The region shares a valuable constitutional heritage that dogmatically protects freedom of expression, access to information, and the right to privacy. However, in practice, the effectiveness of these guarantees is undermined by political and infrastructure barriers, as well as violence. Phenomena such as judicial harassment through anachronistic defamation laws (SLAPPs in Panama and Honduras), systemic violence against the press (Mexico), digital surveillance of journalists, and the use of states of emergency that legalize unrestricted surveillance and encourage self-censorship (El Salvador) demonstrate that the digital civic space is under siege, contravening the “high threshold” of protection required by international law.

2. Need for regulatory progress. The region is clearly lagging behind technology corporations. Except for sector-specific approaches in Mexico (copyright) and Panama (e-commerce), countries lack modern laws that define the role of digital platforms and establish a *safe harbor* regime. This gap forces states to improvise using consumer protection laws or high-tech criminal codes, resulting in a punitive approach toward end users, rather than imposing obligations of due diligence, algorithmic transparency, and appeal mechanisms (due process) on the platforms themselves.

3. Institutional Fragility and Asymmetry in Data Protection. With the exception of Mexico and Panama, which have legislation applicable to the private sector, privacy protection in the region is precarious, relying on the reactive remedy of *Habeas Data* or on laws limited to the public or credit sectors. Added to this is a critical failure to comply with the UNESCO standard on the independence of regulators. Telecommunications authorities are often subordinate to the executive branch. The case of Mexico is particularly concerning, as it recently eliminated the constitutional autonomy of its key regulators (such as the INAI and the IFT), dismantling the basic institutional checks and balances against state intervention.

4. Vulnerability of electoral integrity to disinformation and artificial intelligence. The digital ecosystem has become the main political battleground, outpacing the enforcement and technical capabilities of electoral bodies. While Panama stands out as a regulatory pioneer by banning *bots* and inauthentic accounts and criminalizing the malicious use of AI to spread disinformation, the rest of the region relies on fragile voluntary agreements or finds itself in a complete legal vacuum (such as El Salvador or the Dominican Republic, which are unable to audit micro-targeted foreign advertising). The advent of generative AI threatens to make psychographic manipulation cheaper and more automated, demanding urgent reforms focused on safeguarding the democratic process.

5. Market asymmetry and the need for a regional bloc. One of the most compelling conclusions emerging from the 2025 workshops is that the nations of Central America and the Caribbean, due to the small size of their markets, lack the bargaining power (“diplomatic muscle”) to hold Big Tech companies accountable, compel them to open local offices, or adapt

their automated moderation systems to the region's indigenous languages and dialects (linguistic sovereignty). To overcome this asymmetry, isolated government action is futile; it is essential to move toward the formation of **regional negotiating blocs**.

6. Toward Innovative Governance. Faced with a lack of physical jurisdiction over the platforms, the region must think outside traditional frameworks. As proposed in the inter-institutional dialogues, a highly effective way to compel platforms to comply with human rights standards and mitigate systemic risks is to involve **financial regulatory agencies and tax authorities**. Utilizing control over economic flows (advertising payments, subscriptions, and monetization) provides states with the necessary leverage to demand the transparency and shared responsibility that electoral bodies and other competent authorities have failed to enforce.

12.2 Recommended Actions

The region of Central America, Mexico, and the Caribbean is at a crossroads. To realize the vision of a “trustworthy internet” promoted by UNESCO, governments must move away from punitive and surveillance-based models and embrace systemic, multi-stakeholder governance. This requires granting regulators true independence, modernizing electoral laws, promoting digital literacy to break down information bubbles, and act as a united region that demands platforms adapt their technologies to respect the dignity and human rights of their populations. That said, our research allowed us to identify a series of key areas where civil society and regulators found consensus and on which work can be done.

In this regard, the **I4T Knowledge Network** can collaborate with authorities and civil society organizations in the region and serve as a liaison with UNESCO, providing support, sharing knowledge, technical assistance, and evidence to help countries in the region move toward a governance framework for digital platforms that addresses challenges common to different regions of the world and also responds to the priorities identified in the region.

The key areas and recommended actions are summarized below:

Key Area	Main Findings and Concepts	Recommended Actions
Shift in Regulatory Focus	Consensus on the need to move away from efforts to regulate specific pieces of content (risk of censorship).	Focus on regulating systems and processes , algorithms, moderation policies, and transparency. Do not necessarily seek strict regulation.
Regional Strategy	Individual small nations lack influence against the tech giants	Form regional blocs (Central America and the Caribbean) to gain “diplomatic clout” and achieve regulatory convergence. Be creative: Explore the role of non-traditional authorities, such as banking supervisory agencies.
Electoral Integrity	Digital platforms are major battlegrounds for disinformation and jeopardize electoral processes.	Update national laws to cover digital campaigns and protect democratic processes . Combat dark money in advertising.

Key Area	Main Findings and Concepts	Recommended Actions
Technological Sovereignty	Heavy reliance on foreign infrastructure (cloud, AI) creates vulnerability.	Improve personal data protection and work toward greater regional technological autonomy . (Although this priority has been identified, there are major questions surrounding how it can be achieved.)
Inclusion and Digital Literacy	One-size-fits-all global policies ignore local languages and cultural nuances .	Invest in digital literacy for citizens and require moderation that respects indigenous languages. Work within an international framework .
AI Governance	Generative AI and <i>deepfakes</i> pose systemic risks to dignity and truth.	Develop clear frameworks and safeguards against AI-driven abuses.

13. Bibliography

Álvarez Pinzón, G. P., & Herrera Ortiz, M. (2025). Freedom Not Available: The Setback of Digital Rights in the Face of Administrative Centralization in Mexico. *Journal of Law and Information Technology*, 14(2), 45–68. <https://doi.org/10.1017/rdti.2025.102>

Amnesty International. (January 13, 2022). *El Salvador: Amnesty International verifies the use of the Pegasus spyware to monitor journalists*. <https://www.amnesty.org/es/latest/news/2022/01/el-salvador-pegasus-spyware-surveillance-journalists/>

Amnesty International. (May 2, 2023). *Dominican Republic: The discovery of the Pegasus spyware on a prominent journalist's phone must lead to an impartial investigation*. <https://www.amnesty.org/es/latest/news/2023/05/dominican-republic-discovery-of-pegasus-spyware-on-prominent-journalists-phone/>

Amnesty International. (2025, August 14). *Dominican Republic: New Penal Code fails to guarantee the rights of women and girls*. <https://www.amnesty.org/es/latest/news/2025/08/republica-dominicana-nuevo-codigo-penal-no-garantiza-los-derechos-de-las-mujeres-y-ninas/>

Legislative Assembly of the Republic of Costa Rica. (June 19, 1954). *Law No. 1758. Radio Law*. Official Gazette No. 142.

Legislative Assembly of the Republic of Costa Rica. (October 10, 1975). *Law No. 5811. Law on the Office of Propaganda Control*. Official Gazette No. 202.

Legislative Assembly of the Republic of Costa Rica. (August 30, 2005). *Law No. 8454. Law on Certificates, Digital Signatures, and Electronic Documents*. Official Gazette No. 197.

Legislative Assembly of the Republic of Costa Rica. (June 4, 2008). *Law No. 8642. General Telecommunications Law*. Official Gazette No. 107.

Legislative Assembly of the Republic of Costa Rica. (September 2, 2009). *Law No. 8765. Electoral Code*. Official Gazette No. 171, Supplement No. 37.

Legislative Assembly of the Republic of Costa Rica. (July 7, 2011). *Law No. 8968. Protection of Individuals with Respect to the Processing of Their Personal Data*. Official Gazette No. 170.

Legislative Assembly of the Republic of Costa Rica. (July 11, 2022). *Law No. 10267. Law Prohibiting the Dissemination of Propaganda That Degrades Older Adults*. Official Gazette No. 172.

Legislative Assembly of the Republic of El Salvador. (May 22, 1997). *Decree No. 142. Telecommunications Act*. Official Gazette No. 108, Volume No. 335.

Legislative Assembly of the Republic of El Salvador. (August 31, 2005). *Decree No. 772. Consumer Protection Act*. Official Gazette No. 166, Volume No. 368.

Legislative Assembly of the Republic of El Salvador. (March 4, 2010). *Decree No. 285. Special Law on Telecommunications Interception*. Official Gazette No. 45, Volume No. 386.

Legislative Assembly of the Republic of El Salvador. (November 4, 2010). *Decree No. 555. Provisions for the Nomination of Non-Partisan Candidates in Legislative Elections*. Official Gazette No. 222, Volume No. 389.

Legislative Assembly of the Republic of El Salvador. (April 8, 2011). *Decree No. 534. Law on Access to Public Information*. Official Gazette No. 70, Volume No. 391.

Legislative Assembly of the Republic of El Salvador. (January 31, 2013). *Decree No. 307. Law on Political Parties*. Official Gazette No. 32, Volume No. 398.

Legislative Assembly of the Republic of El Salvador. (July 3, 2013). *Decree No. 413. Electoral Code*. Official Gazette No. 122, Volume No. 400.

Legislative Assembly of the Republic of El Salvador. (October 22, 2015). *Decree No. 133. Electronic Signature Act*. Official Gazette No. 201, Volume No. 409.

Legislative Assembly of the Republic of El Salvador. (February 4, 2016). *Decree No. 260. Special Law Against Cybercrimes and Related Offenses*. Official Gazette No. 29, Volume No. 410.

Legislative Assembly of the Republic of El Salvador. (October 22, 2020). *Decree No. 463. Electronic Commerce Act*. Official Gazette No. 215, Volume No. 429.

Legislative Assembly of the Republic of El Salvador. (March 27, 2022). *Decree No. 333. State of Emergency*. Official Gazette No. 59, Volume No. 434.

Legislative Assembly of the Republic of El Salvador. (June 22, 2022). *Decree No. 431. "Growing Together" Law for the Comprehensive Protection of Infancy, Childhood, and Adolescence*. Official Gazette No. 118, Volume No. 435.

Legislative Assembly of the Republic of El Salvador. (October 18, 2022). *Special Law on Voting Abroad*. Official Gazette No. 197, Volume No. 437.

Legislative Assembly of the Republic of El Salvador. (November 2, 2023). *Deputies Decriminalize the Dissemination of Messages Generated by Gangs*. <https://www.asamblea.gob.sv/node/12992>

National Constituent Assembly of the Republic of El Salvador. (December 15, 1983). *Constitution of the Republic of El Salvador*. Official Gazette No. 234.

National Constituent Assembly of the Republic of Guatemala. (May 5, 1966). *Law on Freedom of Expression*. *Decree No. 9*. Diario de Centro América.

National Constituent Assembly of the Republic of Guatemala. (May 31, 1985). *Political Constitution of the Republic of Guatemala*. Diario de Centro América.

National Constituent Assembly of the Republic of Guatemala. (December 3, 1985). *Law on Elections and Political Parties*. *Decree No. 1-85*. Diario de Centro América.

National Constituent Assembly of the Republic of Guatemala. (January 8, 1986). *Law on Amparo, Personal Appearance, and Constitutionality*. *Decree No. 1-86*. Diario de Centro América.

National Constituent Assembly of the Republic of Honduras. (July 26, 1958). *Law on Freedom of Expression*. *Decree No. 6*. Official Gazette La Gaceta.

National Constituent Assembly of the Republic of Honduras. (January 20, 1982). *Constitution of the Republic of Honduras*. *Decree No. 131*. Official Gazette La Gaceta.

Chamber of Deputies of Mexico. (2024, December 20). *DOF publishes decree on constitutional reform regarding organizational simplification (Note No. 1268)*. Social Communication: News Agency.

Chamber of Information and Communication Technologies (CAESCO). (May 6, 2025). *Preliminary report on the draft Organic Law on Freedom of Expression and Audiovisual Media of the Dominican*

Republic. <https://caesco.org/wp-content/uploads/2025/05/Informe-preliminar-sobre-el-Proyecto-de-Ley-Libertad-de-Expresion.pdf>

Calderón, S. (October 15, 2024). More than 50% of Salvadorans spend more than three hours a day on social media. *Diario El Mundo*. <https://diario.elmundo.sv/economia/mas-50-de-los-salvadorenos-pasa-mas-de-tres-horas-diarias-en-redes-sociales>

Cebrián Zazurca, E. (2016). The Impact of the Internet on the Democratic State. *Journal of Political Studies*, (173), 307–320.

Center for Transdisciplinary Studies in Central America. (2023, September 27). *Authoritarianism in Central America: Illegitimate Criminal Prosecution in Guatemala, El Salvador, Honduras, and Nicaragua*. <https://www.cetcam.org/los-autoritarismos-en-centroamerica-promueven-la-persecucion-penal-ilegitima/>

Chivo Wallet. (n.d.). *Home*. Retrieved February 25, 2026, from <https://www.chivowallet.com/>
Inter-American Commission on Human Rights. (August 14, 2025). *El Salvador: IACHR reiterates concern over the excessive prolongation and improper application of the state of emergency*. Organization of American States. <https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2025/162.asp>

National Telecommunications Commission of Honduras. (August 23, 2011). *Regulations Governing Internet Service or Access to Computer Networks*. Resolution No. NR004/11. Official Gazette, La Gaceta.

Committee to Protect Journalists. (April 8, 2022). *New law adopted in El Salvador imposes prison sentences of up to 15 years on journalists who report on gangs*. <https://cpj.org/es/2022/04/nueva-ley-adoptada-en-el-salvador-sanciona-con-penas-de-hasta-15-anos-de-prision-a-los-periodistas-que-den-cobertura-informativa-a-las-pandillas/>

Mexico City Congress. (June 7, 2024). *Code of Electoral Institutions and Procedures of Mexico City*. Official Gazette of Mexico City.

Congress of the Republic of Guatemala. (July 1, 1992). *Value-Added Tax Law*. Decree No. 27-92. Diario de Centro América.

Congress of the Republic of Guatemala. (October 17, 1996). *General Telecommunications Law*. Decree No. 94-96. Diario de Centro América.

Congress of the Republic of Guatemala. (July 18, 2003). *Comprehensive Protection of Children and Adolescents Act*. Decree No. 27-2003. Diario de Centro América.

Congress of the Republic of Guatemala. (September 23, 2008). *Law on Access to Public Information*. Decree No. 57-2008. Diario de Centro América.

Congress of the Republic of Guatemala. (July 8, 2025). *Bill to Approve the Law on the Protection of Personal Data*. Bill No. 6572. Legislative Directorate.

National Congress of Honduras. (October 31, 1995). *Framework Law on the Telecommunications Sector*. Decree No. 185-95. Official Gazette La Gaceta.

National Congress of Honduras. (December 30, 2006). *Law on Transparency and Access to Public Information*. Decree No. 170-2006. Official Gazette, La Gaceta.

National Congress of Honduras. (July 7, 2008). *Consumer Protection Act*. Decree No. 24-2008. Official Gazette, La Gaceta.

National Congress of Honduras. (December 12, 2011). *Special Law on the Interception of Private Communications. Decree No. 243-2011*. Official Gazette, La Gaceta.

National Congress of Honduras. (December 11, 2013). *Law on Electronic Signatures. Decree No. 149-2013*. Official Gazette, La Gaceta.

National Congress of Honduras. (October 18, 2017). *Penal Code of Honduras. Decree No. 130-2017*. Official Gazette La Gaceta.

National Congress of Honduras. (May 26, 2021). *Electoral Law of Honduras. Decree No. 35-2021*. Official Gazette No. 35,609.

National Council for Financial Inclusion and Education of El Salvador. (n.d.). *Bitcoin in El Salvador*. Retrieved February 25, 2026, from <https://inclusionfinanciera.gob.sv/bitcoin-en-el-salvador/>

Latinobarómetro Corporation. (2020). *2020 Report*. <https://www.latinobarometro.org/latOnline.jsp>
Constitutional Court of Guatemala. (October 14, 2004). *Ruling on Case No. 1822-2003*.

Inter-American Court of Human Rights. (November 13, 1985). *Mandatory membership in a professional association for journalists (Arts. 13 and 29 of the American Convention on Human Rights)* (Advisory Opinion OC-5/85, Series A No. 5). <https://www.corteidh.or.cr/tablas/a12040.pdf>

Inter-American Court of Human Rights. (February 6, 2001). *Case of Ivcher Bronstein v. Peru* (Judgment on the Merits, Reparations, and Costs, Series C No. 74). https://www.corteidh.or.cr/docs/casos/articulos/seriec_74_esp.pdf

Inter-American Court of Human Rights. (February 5, 2001). *Case of "The Last Temptation of Christ" (Olmedo Bustos et al.) v. Chile* (Judgment on the Merits, Reparations, and Costs, Series C No. 73).

Inter-American Court of Human Rights. (July 2, 2004). *Case of Herrera Ulloa v. Costa Rica* (Judgment on Preliminary Objections, Merits, Reparations, and Costs, Series C No. 107).

Inter-American Court of Human Rights. (August 31, 2004). *Case of Ricardo Canese v. Paraguay* (Judgment on the merits, reparations, and costs, Series C No. 111).

Inter-American Court of Human Rights. (November 22, 2005). *Case of Palamara Iribarne v. Chile* (Judgment on the merits, reparations, and costs, Series C No. 135).

Inter-American Court of Human Rights. (September 19, 2006). *Case of Claude Reyes et al. v. Chile* (Judgment on the Merits, Reparations, and Costs, Series C No. 151).

Cubilla-Bonnetier, D., Grajales-Barrios, M., Ortega-Espinosa, A., Puertas, L., and De León Sautú, N. (February 6, 2023). Unequal literacy development and access to online education in public versus private Panamanian schools during the COVID-19 pandemic. *Frontiers in Education*, 8. <https://doi.org/10.3389/feduc.2023.989872>

DataReportal. (n.d.). *Global digital insights*. Retrieved August 27, 2025, from <https://datareportal.com/>

Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (1998). <https://www.copyright.gov/legislation/dmca.pdf>

General Directorate of Internal Revenue of the Dominican Republic. (August 17, 2023). *General Regulation No. 07-2023 on the Registration and Administration of Digital Service Providers*.

- Freedom House. (May 31, 2024). *Freedom on the Net 2024: Mexico*. <https://freedomhouse.org/country/mexico/freedom-net/2024>
- Freedom House. (2025). *Freedom in the World 2025: Panama*. <https://freedomhouse.org/country/panama>
- Galpaya, H. (February 23, 2017). *Zero-rating in emerging economies* (Global Commission on Internet Governance Paper Series No. 47). Centre for International Governance Innovation.
- Gordón Guerrel, I. (November 22, 2025). Electoral Reform Commission to be extended until 2026. *La Estrella de Panamá*.
- Graña Gianoni, J. (April 2025). *Challenges to freedom of expression, the rule of law, and democracy in Latin America: A regional study on SLAPPs*. Panama. Baltasar Garzón International Foundation (FIBGAR).
- Guerrero Rodríguez, O. (July 2, 2025). *Reforms to the Federal Economic Competition Law and the Abolition of COFECE and IFT*. Hogan Lovells.
- Herrera, K. (2022). *Active Social Media Users in Costa Rica: Overall Geographic Distribution, Age, and Gender* [Infographic]. Snapshot of the Connected Consumer, El Financiero.
- Human Rights Watch. (2024). *World Report 2024: El Salvador*. Retrieved February 25, 2026, from <https://www.hrw.org/es/world-report/2024/country-chapters/el-salvador>
- Human Rights Watch. (2024). *World Report 2024: Guatemala*. <https://www.hrw.org/es/world-report/2024/country-chapters/guatemala>
- Dominican Institute of Telecommunications. (December 14, 2021). *Resolution No. 126-2021 establishing the Cybersecurity Regulations for the Provision of Internet Access Services*.
- National Institute of Statistics, Geography, and Informatics of Mexico. (2024). *National Survey on the Availability and Use of Information Technologies in Households (ENDUTIH) 2024*.
- International IDEA. (2025). *Democracy Tracker: Panama*. <https://www.idea.int/democracytracker/country/panama>
- International Telecommunication Union. (August 2023). *Digital Development Dashboard BETA: El Salvador*.
- International Trade Administration. (2024). *El Salvador - Information and Communications Technology*. U.S. Department of Commerce.
- Internet Society. (2026). *Country report for El Salvador*. Internet Society Pulse. Retrieved February 25, 2026.
- Kemp, S. (February 2024). *Digital 2024: Guatemala*. DataReportal.
- Kemp, S. (February 2024). *Digital 2024: Honduras*. DataReportal.
- Kemp, S. (February 2024). *Digital 2024: Mexico*. We Are Social; Kepios.
- Kemp, S. (January 2025). *Digital 2025: Costa Rica*. DataReportal.
- Kemp, S. (January 2025). *Digital 2025: Guatemala*. DataReportal.
- Kemp, S. (December 15, 2025). *Digital 2026: Panama*. DataReportal; Kepios.

Kemp, S. (November 8, 2025). *Digital 2026: El Salvador*. DataReportal.

Kepios / DataReportal. (2025). *Digital 2025: The Dominican Republic*.

La Prensa. (February 21, 2024). *Honduras Reaches 4.5 Million Social Media Users in 2024*.

López de Ramos, A. L., Casado Robles, E., Atagua-Díaz, Z., Prado, J. F., Álvarez Franco, A. M., Cáceres, A., and Ramos Fortuna, V. (2024). Analysis of Digital Literacy: Exploring the Gender Gap Among Panamanian College Students. *Latitude*, 1(19), 22–46. <https://doi.org/10.55946/latitude.v1i19.242>

Márquez, D. (2025, June 10). *DataReportal and Internet and Social Media Use in El Salvador 2025*. iLifebelt.

Massé, E., Björkstén, & Chima, R. J. S. (June 4, 2016). *Zero rating: A global threat to the open internet*. Access Now.

McSherry, C. (September 16, 2020). *Notice and takedown mechanisms: Risks for freedom of expression online* [Written statement]. Electronic Frontier Foundation.

Méndez Dardón, A. M. (2022). Freedom of expression in Guatemala: between repression and resistance. *Journal of Political Science at Rafael Landívar University*, 15(2), 45–67.

Mexico. (February 5, 1917). *Political Constitution of the United Mexican States*. Official Gazette of the Federation.

Mexico. (2020, July 1). *Federal Copyright Law*. Official Gazette of the Federation.

Mexico. (December 16, 2024). *General Law on Women's Access to a Life Free of Violence*. Official Gazette of the Federation.

Mexico. (December 20, 2024). *Decree Amending, Supplementing, and Repealing Various Provisions of the Political Constitution of the United Mexican States Regarding Organizational Simplification*. Official Gazette of the Federation.

Mexico. (December 26, 2024). *Federal Consumer Protection Law*. Official Gazette of the Federation.

Mexico. (February 21, 2025). *Federal Labor Law*. Official Gazette of the Federation.

Mexico. (2025, March 20). *Federal Law on the Protection of Personal Data Held by Private Parties*. Official Gazette of the Federation.

Mexico. (July 16, 2025). *Federal Economic Competition Law*. Official Gazette of the Federation.

Mexico. (2025, July 16). *Federal Telecommunications and Broadcasting Law*. Official Gazette of the Federation.

Mexico. (November 28, 2025). *Federal Criminal Code*. Official Gazette of the Federation.

Mexico. Government of the Republic. (2017). *National Cybersecurity Strategy*.

Mindus, P. (2014). What does “e-” add to democracy?: Designing an agenda for democracy theory in the information age. In J. Bishop (Ed.), *Transforming politics and policy in the digital age*.

- Ministry of Finance of Costa Rica. (2025). *VAT Collection on Cross-Border Digital Services*. General Directorate of Taxation.
- Ministry of Women of the Dominican Republic. (2024). *Innovation in Legislative Proposals for the Eradication of Gender-Based Violence*.
- Joint mission by Freedom House, ARTICLE 19, CPJ, RSF, et al. (2023). *Report on the findings of the international mission on freedom of the press and freedom of expression in Guatemala*.
- Mondragón Toledo, G. (2015). *The Importance of the Internet as a Source of Power in Society*. University of Murcia.
- Movimiento Puente. (n.d.). Honduras: Digital Rights. <https://derechosdigitales.movpuente.com/honduras/>
- OECD. (2023). *PISA 2022 Results (Volume I): The State of Learning and Equity in Education*. OECD Publishing. <https://doi.org/10.1787/53f23881-en>
- UN. (July 19, 2021). *Governments cannot use technologies to spy on citizens that violate human rights*. United Nations.
- Opensignal. (December 2024). *Costa Rica Mobile Network Experience Report*.
- Opensignal. (March 2025). *Guatemala: Mobile Network Experience Report*.
- United Nations. (December 16, 1966). *International Covenant on Civil and Political Rights*. Treaty Series, 999, 171.
- Organization of American States. (November 22, 1969). *American Convention on Human Rights*. O.A.S.T.S. No. 36.
- Panama. (July 12, 1962). *Executive Decree No. 155, Code of Ethics and Professional Responsibility for Attorneys*. Official Gazette No. 14,672.
- Panama. (1972). *Political Constitution of the Republic of Panama*. Official Gazette No. 17,210. (Updated with 2004 amendments).
- Panama. (February 9, 1996). *Law 31 of 1996: Regulation of Telecommunications*. Official Gazette No. 22,971.
- Panama. (June 30, 1999). *Law No. 24 of 1999: Public Radio and Television Services*. Official Gazette No. 23,832.
- Panama. (January 22, 2002). *Law No. 6 of 2002: Transparency in Public Administration and Habeas Data*. Official Gazette No. 24,476.
- Panama. (July 22, 2008). *Law No. 51 of 2008: Electronic Documents, Electronic Signatures, and E-commerce*. Official Gazette No. 26,090.
- Panama. (August 11, 2008). *Law No. 59 of 2008: Universal Service and Access to Telecommunications*. Official Gazette No. 26,106.
- Panama. (October 10, 2012). *Law No. 44 of 2012: Copyright and Related Rights*. Official Gazette No. 27,141.

- Panama. (November 14, 2013). *Law No. 79 of 2013: Approves the Convention on Cybercrime (Budapest)*. Official Gazette No. 27,415.
- Panama. (October 24, 2013). *Law No. 82 of 2013: Measures against violence against women and criminalization of femicide*. Official Gazette No. 27,401.
- Panama. (March 26, 2019). *Law No. 81 of 2019: Protection of Personal Data*. Official Gazette No. 28,743-A.
- Panama. (May 14, 2019). *Penal Code of the Republic of Panama (Consolidated Text)*. Official Gazette No. 28,774-B.
- Panama. (October 22, 2021). *Law No. 247 of 2021: Amendment to the Electoral Code*. Official Gazette No. 29,403-A.
- Panama. (October 28, 2022). *Consolidated Text of the Electoral Code (Decree 60 of 2022)*. Official Gazette No. 29,652-A.
- Panama. (January 23, 2024). *Executive Decree No. 7 of 2024: Regulates Law 81 on the Protection of Personal Data*. Official Gazette No. 29,956-B.
- Piña, G. (July 11, 2025). Opaque Mexico: Lack of Transparency and Media Crackdown. *Diálogo Político*.
- Executive Branch of the Republic of Costa Rica. (August 4, 1954). *Executive Decree No. 18. Regulations for the Radio Law*. Official Gazette No. 175.
- Executive Branch of the Republic of Costa Rica. (2013, March 5). *Executive Decree No. 37541-JP. Regulations for the Law on the Protection of Individuals with Regard to the Processing of Their Personal Data*. Official Gazette No. 45.
- United Nations Development Program. (April 15, 2025). *Data in the Cloud, Centers on Earth: The Role of Data Centers in the Digital Future of Latin America and the Caribbean*. <https://www.undp.org/es/latin-america/blog/datos-en-la-nube-centros-en-la-tierra-el-rol-de-los-centros-de-datos-en-el-futuro-digital-de-alc>
- Program on Freedom of Expression, Right to Information, and Public Opinion (PROLEDI). (n.d.). *PROLEDI Publications*. University of Costa Rica. Retrieved March 3, 2026, from <https://proledi.ucr.ac.cr/publicaciones-proledi/>
- Pulso Capital. (2025, June 16). *Internet and Social Media Use in El Salvador 2025*. <https://pulsocapital.com/uso-de-internet-redes-sociales-el-salvador-2025/>
- Raziel, Z. (April 25, 2025). Sheinbaum Puts the Telecommunications Law on Hold Following Controversy Over the Provision Allowing the Government to Block Digital Platforms. *El País*.
- RED 506. (2022). *RED 506 Infographics* [Slides]. SlideShare.
- Special Rapporteur for Freedom of Expression. (2017). *Standards for a Free, Open, and Inclusive Internet*. Inter-American Commission on Human Rights.
- Special Rapporteur on Freedom of Expression. (2025). *The Impact of Digital Surveillance on Freedom of Expression in the Americas* (OEA/Ser.L/V/II/CIDH/RELE/INF.33/25).
- Reporters Without Borders. (2023). *Dominican Republic: Economic Context*. <https://rsf.org/es/pais/republica-dominicana>

Reporters Without Borders. (2025, May 2). 2025 World Press Freedom Index. <https://rsf.org/es/clasificacion>

Dominican Republic. (December 15, 1962). *Law No. 6132 on the Expression and Dissemination of Thought*. Official Gazette No. 8,725.

Dominican Republic. (January 27, 1997). *Law No. 24-97: Amendments to the Penal Code and Protection of Children*. Official Gazette No. 9,945.

Dominican Republic. (May 27, 1998). *General Telecommunications Law (Law No. 153-98)*. Official Gazette No. 9,983.

Dominican Republic. (September 4, 2002). *Law No. 126-02 on Electronic Commerce, Digital Documents, and Digital Signatures*. Official Gazette No. 10,172.

Dominican Republic. (August 7, 2003). *Law No. 136-03: Code for the Protection System and Fundamental Rights of Children and Adolescents*. Official Gazette No. 10,234.

Dominican Republic. (July 28, 2004). *General Law on Free Access to Public Information (Law No. 200-04)*. Official Gazette No. 10,290.

Dominican Republic. (April 23, 2007). *Law No. 53-07 on High-Tech Crimes and Offenses*. Official Gazette No. 10,416.

Dominican Republic. (December 15, 2013). *Law No. 172-13: Comprehensive Protection of Personal Data*. Official Gazette No. 10,737.

Dominican Republic. (June 13, 2015). *Constitution of the Dominican Republic*. Official Gazette No. 10,805.

Dominican Republic. (August 13, 2018). *Law No. 33-18 on Political Parties, Groups, and Movements*. Official Gazette No. 10,917.

Dominican Republic. (June 14, 2022). *Decree No. 313-22: National Cybersecurity Strategy 2030*. Official Gazette No. 11,069.

Dominican Republic. (February 17, 2023). *Law No. 20-23: Organic Law on the Electoral System*. Official Gazette No. 11,092.

Dominican Republic. (October 11, 2023). *Decree No. 498-23: National Artificial Intelligence Strategy (ENIA)*. Official Gazette No. 11,109.

Dominican Republic. (January 15, 2024). *Law No. 1-24: National Intelligence Directorate (DNI)*. Official Gazette No. 11,156.

Dominican Republic. (August 15, 2025). *Law No. 74-25 establishing the Penal Code of the Dominican Republic*. Official Gazette No. 11,124.

Reuters Fact Check. (May 27, 2024). *Fact Check: French university did not conduct studies predicting the outcome of the Mexican elections*.

Riquelme, R. (May 6, 2025). 100 million people already use the internet in Mexico: INEGI. *El Economista*.

Constitutional Chamber of the Supreme Court of Justice of Costa Rica. (2024). *Annual Statistical Compendium*.

Sensor Tower. (2024). *Top Social Networking Apps in Guatemala, Q3 2024*.

Shum, Y. (February 16, 2023). *Digital Landscape, Internet, and Social Media in Honduras 2023*.

Inter-American Press Association. (April 2024). *Dominican Republic Report to the Mid-Year Meeting*. <https://www.sipiapa.org/notas/1216584-republica-dominicana>

Inter-American Press Association. (July 4, 2024). *The IAPA Welcomes the Supreme Court Ruling Strengthening Freedom of Expression in Panama*.

Costa Rican Telecommunications Superintendency (SUTEL). (2024). *2024 Telecommunications Sector Statistics*.

Teleread. (2025). *News and updates on the electronic payment system in Panama*.

Thomson Reuters. (February 28, 2024). El Salvador grants Musk's Starlink unit a concession for satellite internet. *COOL FM*.

Constitutional Court of the Dominican Republic. (February 19, 2016). *Ruling TC/0075/16 (Unconstitutionality of Articles of Law 6132)*.

Supreme Electoral Tribunal of the Republic of Costa Rica. (2025, June 20). *Resolution No. 4190-E8-2025: Use of institutional digital platforms during campaigns*.

Supreme Electoral Tribunal of the Republic of Guatemala. (October 12, 2016). *Regulations to the Electoral and Political Parties Law. Agreement No. 435-2016*.

Supreme Electoral Tribunal of the Republic of Guatemala. (2018, January 19). *Regulations of the Specialized Unit on Media and Opinion Polls. Agreement No. 15-2018*.

Ulate Chacón, E. N. (2015). *From Central American Constitutional Heritage to Central American Constitutional Law: Studies in Comparative Law*. ISOLMA.

UNESCO. (September 28, 2024). *Transparency and Access to Public Information in Latin America and the Caribbean: Pillars of Democracy*.

University of Costa Rica. (2025). *Report on Displaced Voices*. PROLEDI.

U.S. Department of State. (2025). *2024 Country Reports on Human Rights Practices: Panama*. Bureau of Democracy, Human Rights, and Labor.

V-Dem. (2025). *Freedom of Expression Index - V-Dem [Dataset]*. Our World in Data.

Vesco Consultores. (May 8, 2024). *Taxation of Digital Platforms in Guatemala*.

WePlan Analytics. (September 2024). *Costa Rica Mobile Quality Report*.

Proyecto apoyado por:

