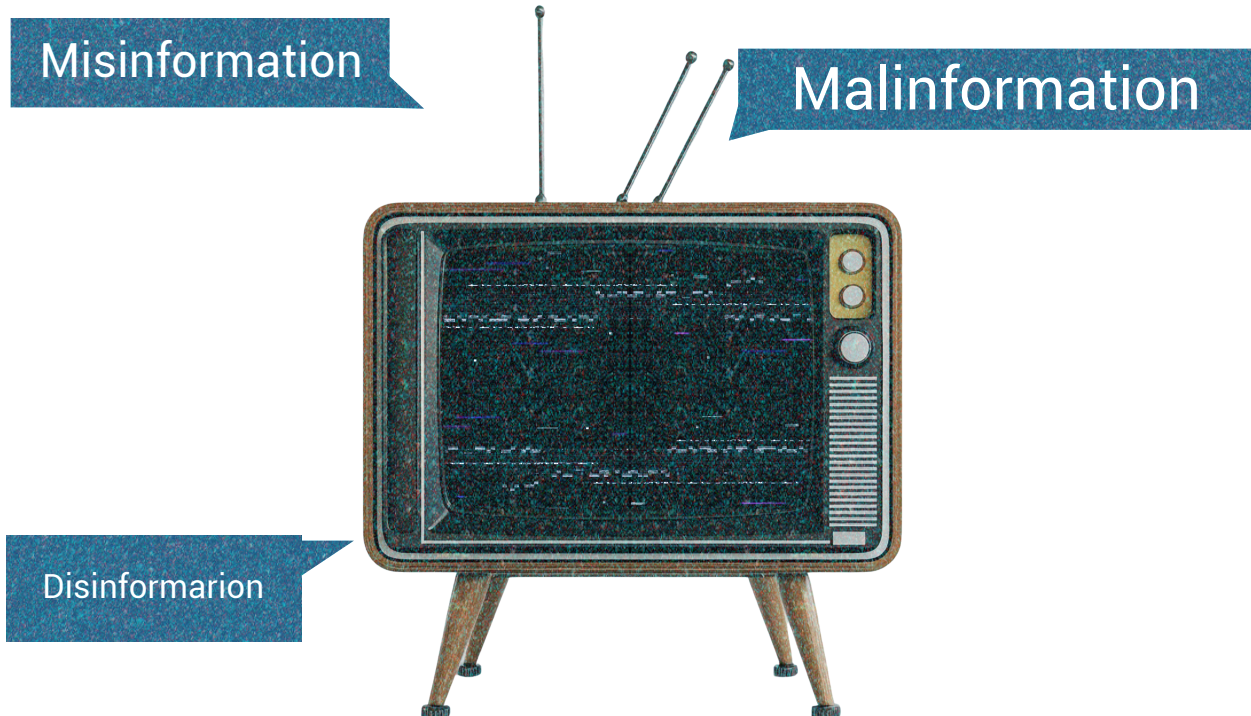




Countering Misinformation, Disinformation, and Malinformation (MDM) Practices in Lebanon

This Policy Brief was created by the Lebanese Center for Human Rights (CLDH) as part of the "Safeguarding Human Rights Amid Crisis in Lebanon" project, funded by the United Nations Democracy Fund (UNDEF)



Contents



Overview & Definitions



Undermining Rights: How MDM Practices Breach National and International Protections



Regulating Misinformation and Digital Manipulation (MDM): Legal Gaps and the Role of Internal Policies



Recommendations

1 Overview & Definitions

Overview:

When we talk about Misinformation, Disinformation, and Malinformation (MDM), we are referring to a growing phenomenon shaped by the rapid evolution of digital communication and information exchange. These practices represent new forms of information distortion that frequently evade traditional regulatory and legal frameworks. While MDM often unfolds in the digital sphere, its consequences are deeply tangible—fueling discrimination, infringing on personal rights, and undermining democratic trust in institutions. The difficulty in addressing MDM lies not only in its unprecedented speed and scale but in its ability to exploit legal grey areas and outdated regulatory models.

Definitions:

MDM practices differ in both intent and impact.

- 1 Misinformation** Misinformation refers to the unintentional spread of false or inaccurate information, whereas disinformation is the deliberate dissemination of false content to deceive or manipulate.
- 2 Disinformation** Disinformation is the intentional creation and dissemination of false information with the aim of deceiving, manipulating, or influencing public opinion. This may involve fabricated news stories, doctored images, or orchestrated campaigns, often serving political, economic, or ideological agendas.
- 3 Malinformation** Malinformation, by contrast, involves the use of verified information in a misleading context or with harmful intent. Together, these categories form a complex and evolving ecosystem of digital manipulation that has far-reaching consequences for democratic participation, public safety, and human dignity.

In Lebanon, established media institutions have struggled to act as safeguards against false information but have often served as active conduits of MDM. On these platforms, public figures have, at times, amplified baseless claims or incited discriminatory behavior against vulnerable communities, including refugees, LGBTQ+ individuals, and civil society actors. These practices have led to real-world consequences—ranging from public defamation to physical violence—revealing the urgent need for accountability in the media landscape.

This policy brief is primarily concerned with identifying the legal frameworks currently in force, while also highlighting regulatory gaps in Lebanon's approach to MDM. It sets forth practical short- and long-term recommendations with achievable goals for monitoring and regulating MDM practices—whether they occur in the digital sphere or through traditional media outlets—drawing on both local needs and international models.

Within this context, MDM practices in Lebanon cannot be understood solely as isolated incidents of false content. Rather, they must be seen as symptoms of deeper structural weaknesses in media governance, regulatory enforcement, and digital literacy—issues that demand coordinated responses grounded in both legal reform and institutional accountability.

Within this context, MDM practices in Lebanon cannot be understood solely as isolated incidents of false content. Rather, they must be seen as



symptoms of deeper structural weaknesses in media governance, regulatory enforcement, and digital literacy—issues that demand coordinated responses grounded in both legal reform and institutional accountability.

II Undermining Rights: How MDM Practices Breach National and International Frameworks

MDM is a practice that contributes to the violation of fundamental rights protected under both national and international legal frameworks, including the Lebanese Constitution. Below we will outline key articles and laws provides illustrative cases where MDM practices directly contributed to their infringement: On freedom of expression, assembly and association:

Article 13 of the Lebanese Constitution explicitly guarantees the freedoms of opinion, expression, the press, assembly, and association. Despite this constitutional protection, misinformation campaigns have been systematically used to obstruct the exercise of these rights by certain groups.

During the summer of 2023, a targeted hate campaign based on false and misleading information that was gradually framed through religious and political incitement, often attempting to associate homosexuality with moral and sexual deviation. was propagated by a number of political figures and religious leaders against the LGBTIQ+ community in Lebanon. This incitement led to a physical attack by the extremist group “Jnoud el Rab” on a bar in Beirut in August 2023.

● On the right to dignity and protection of reputation:

The Universal Declaration of Human Rights (UDHR), to which Lebanon has adopted, states in Article 12: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.”

Once again, however, misinformation campaigns and MDM practices in general have been instrumental in undermining the rights guaranteed by this article.

A prominent example is the case of Ziad Itani, who was falsely accused of treason in a state-backed disinformation campaign. This campaign involved the dissemination of false criminal allegations resulting in severe reputational damage, and amounting to a violation of Lebanon's commitments under international human rights law.

◆ On the right to privacy and protection from unlawful surveillance:

In response to repeated calls for clear regulations on official surveillance and to protect individuals' privacy, Lebanon passed Law No. 140 on October 27, 1999. This law guarantees the confidentiality of all forms of communication. The law outlines how and when communications can be legally intercepted, whether through a court decision or an administrative order. It also imposes penalties for illegal surveillance and establishes an independent body to ensure that any interception based on administrative orders complies with the law.

In clear violation of this right, as highlighted in this Human Rights Watch report, the Lebanese security agencies have employed social media platforms and dating applications to entrap, extort, and detain LGBTIQ+ individuals. Victims have faced public outings, job loss, mental health challenges, and social exclusion.

III Regulating Misinformation and Digital Manipulation: Legal Gaps and the Role of Internal regulations

The growing prevalence of Misinformation, Disinformation, and Malinformation in Lebanon underscores a critical gap in the country's legal and regulatory landscape. While these practices increasingly infringe on fundamental rights—ranging from freedom of expression to privacy and dignity—there remains no dedicated legal framework in place to address or mitigate their impact. At the same time, attempts to introduce sweeping legislation risk being misused to silence dissent, restrict free speech, and criminalize legitimate criticism. This section outlines the legal vacuum surrounding MDM in Lebanon, identifies existing legal tools that can partially address digital manipulation and emphasizes the importance of internal regulatory policies—particularly those modeled on international standards such as the GDPR and the Digital Services Act—as immediate and rights-respecting responses to these emerging threats.

1 Absence of a general legal framework regulating MDM

There is currently no specific legal framework in Lebanon that directly addresses the issue of misinformation, disinformation, or malinformation. Moreover, introducing a general law to regulate MDM presents a staggering list of challenges and pitfalls. If introduced, these regulations could easily be abused to restrict freedom of expression, limit free speech, and crack down on dissenting political views. Any attempt to regulate this area must therefore be carefully balanced to avoid infringing on fundamental rights.

However, one of the main legal instruments that can be considered as a starting point for addressing MDM at the national level is Law No. 81 of 2018, known as the Electronic Transactions and Personal Data Law. This law was enacted to regulate electronic transactions and protect personal data. While it does not explicitly define or target MDM, some of its provisions are relevant to this issue.

In particular, the law criminalizes:

- Unauthorized access to personal data,
- Forgery of electronic documents, and
- Misuse of information technology (IT) systems.

These provisions can be applied in situations where false or misleading information is spread through electronic means, particularly in relation to the tampering with electronic records, creating forged documents, or unlawfully accessing data to disseminate harmful content.

Although this law does not offer a comprehensive solution to the challenges posed by MDM, it provides certain legal tools that can be used to address specific forms of digital misconduct related to the spread of false information.

2 The importance of internal regulations addressing MDM

The absence of tailored national legislation addressing MDM does not preclude organizations from implementing regulatory measures. In fact, it is advisable for entities such as organizations, syndicates, and corporations to incorporate provisions related to MDM within their internal policies and regulations.

For instance, the European Union's General Data Protection Regulation (GDPR), enacted in 2018, governs the collection, processing, and storage of personal data of individuals within the EU. The GDPR aims to enhance individuals' control over their personal information by:

- Requiring transparency from organizations regarding the use of personal data.

- Requiring transparency from organizations regarding the use of personal data.
- Ensuring informed consent to prevent unauthorized personal targeting and surveillance.
- Granting individuals' rights to access, correct, and delete their data, thereby mitigating the misuse of information.

While MDM often involves the misuse of personal data to target individuals with deceptive, manipulated, or sensitive content—including the unauthorized sharing of intimate or private material—the GDPR addresses these concerns through its stringent data protection provisions.

Additionally, the European Union's Digital Services Act (DSA), enacted in 2022, seeks to create a safer and more transparent online environment. The DSA addresses MDM by:

- Combating illegal content and disinformation through monitoring and removal obligations for online platforms.
- Introducing restrictions on targeted advertising, particularly prohibiting profiling based on sensitive data, which can be exploited in manipulative campaigns.
- Mandating transparency from platforms about their recommendation systems to prevent the amplification of misleading or manipulative content.

In the absence of clear national data protection legislation, it is prudent for organizations to reference recognized standards such as the GDPR and DSA when formulating internal policies related to MDM. These frameworks offer widely accepted provisions and serve as valuable references for best practices concerning the collection, processing, storage, and sharing of personal information, thereby ensuring the protection of individuals' rights as a primary consideration.

IV Recommendations



In addition to identifying legal and regulatory gaps, this paper seeks to outline concrete and actionable steps to counter the rise of MDM practices in Lebanon. Drawing on successful international models—particularly from the European Union—these recommendations are adapted to the Lebanese context and are structured across short-, medium-, and long-term timeframes.

Short Term recommendations:

In the absence of specific national legislation addressing MDM, organizations, syndicates, and corporations should proactively develop and implement internal policies that incorporate MDM-related provisions. The below present an outline on how to advance frameworks that govern digital spheres Design policies that include clear definitions for content manipulation, disinformation, and unauthorized data use.

- Establish ethical standards for digital engagement and content production.
- Design and internal accountability mechanisms to address violations.
- Reference established international models:

Organizations should adopt best practices from international regulatory frameworks, notably the EU's General Data Protection Regulation (GDPR) and Digital Services Act (DSA). These frameworks offer ready-made models that can be adapted for internal governance:

For example, the GDPR emphasizes informed consent, data transparency, and protection from unauthorized targeting—relevant safeguards in combating MDM that exploits personal data.

The DSA requires platforms to monitor and limit the spread of illegal and misleading content, and intro-

duces transparency obligations related to recommendation systems—an approach that can be emulated by media and digital content producers.

- Initiate multi-stakeholder dialogue:

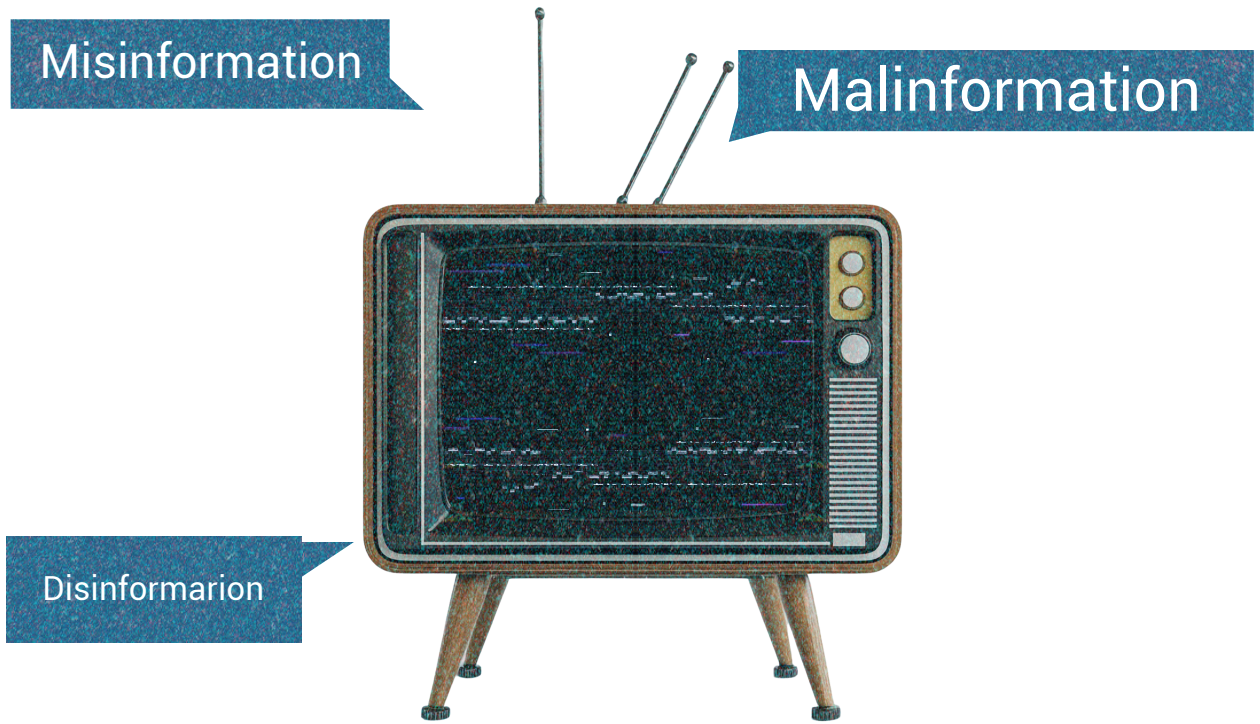
In the short term, civil society, media actors, legal experts, and technologists should come together to form a national working group focused on MDM. This body can serve to share knowledge and monitor trends in MDM across Lebanon; develop draft codes of conduct or voluntary guidelines that can evolve into binding policy; and advocate for safe legislative pathways that avoid censorship and protect freedom of expression.

Medium Term recommendations:

While significant progress has been made in developing media literacy and fact-checking curricula, particularly in private schools, and in training educators across the region, there remains a critical need for the Ministry of Education, in coordination with relevant curriculum development and quality assurance bodies, to ensure the systematic integration and implementation of these courses across public schools and universities. Addressing current funding and resource gaps will be essential to achieving equitable access and nationwide impact.

Long Term recommendations:

Building on existing efforts—such as the development of the Media and Digital Media Information Literacy (MIL/DMIL) curriculum and the training of university instructors and school teachers—the Ministry of Information, Ministry of Education, and media outlets, in collaboration with expert NGOs, should prioritize the development and implementation of a comprehensive national strategy that not only raises public awareness but also advances the adoption of a legal framework specifically designed to regulate MDM practices. This strategy must include both long-term public education and enforceable protections against the spread and harmful use of false, misleading, or manipulated information.



Countering Misinformation, Disinformation, and Malinformation (MDM) Practices in Lebanon

This Policy Brief was created by the Lebanese Center for Human Rights (CLDH) as part of the "Safeguarding Human Rights Amid Crisis in Lebanon" project, funded by the United Nations Democracy Fund (UNDEF)