ADDICTION & SOCIAL MEDIA COMMUNICATION

University of Messina - Journal homepage: https://cab.unime.it/journals/index.php/ASMC/
Addiction & Social Media Communication, 2025, Vol.2, No.2, pag: 3-20

Misinformation, Disinformation and Infodemic: Public Administration's challenges in the digital society

Christian Di Falco [1*], **Caterina Maria Moricca**.[2]

[1] University of Palermo, Department of political science and international relations; [2] Italian Ministry of the Interior – Register of Municipal and Provincial Secretaries

ABSTRACT

Background: The rapid spread of misinformation, disinformation, and infodemic has profoundly reshaped the public communication ecosystem, undermining institutional credibility and citizens' trust. These phenomena, while distinct in nature, converge in weakening the ability of Public Administration to manage accurate, transparent, and effective communication. Understanding their epistemological and operational interconnections is essential to strengthen digital trust and institutional resilience.

Method: The study adopts the theoretical framework of *diagnostic* and *prognostic framing* to conceptually analyze how misinformation, disinformation, and infodemic emerge and interact within contemporary communication systems. The analysis integrates insights from international literature with empirical examples, linking informational distortions to the communicative, regulatory, and organizational challenges faced by public institutions.

Results: The findings reveal that misinformation, disinformation, and infodemic differ in their nature - error, manipulative intent, and information overload - but generate convergent effects: cognitive confusion, social polarization, and erosion of institutional trust. The study identifies strategic responses based on transparency, timeliness, content validation, media literacy, technological monitoring, and inter-institutional cooperation.

Conclusion: Addressing misinformation and disinformation requires a systemic approach that combines regulatory, communicative, and educational dimensions. Public Administration must act both as a guardian against disinformation and as a proactive promoter of transparent and reliable institutional communication. Strengthening institutional resilience and digital trust emerges as a crucial public value for democratic governance.

Keywords: *Misinformation*, *Disinformation*, *Infodemic*, *Public Administration*, *Digital trust*, *Public communication*

* *Corresponding author*: Christian Di Falco - University of Palermo
E-mail address: christian.difalco@unipa.it

doi https:// 10.13129/3035-1383/asmc-5275

Introduction

Assigning a name to a social phenomenon represents a fundamental analytical step: it allows scholars and institutions to delineate its boundaries, identify its causes, and direct resources toward appropriate solutions. In doing so, it helps distinguish what deserves priority intervention from what risks being overlooked. In the literature on social movements, this process is known as *diagnostic framing*, namely the identification and definition of a problem and the recognition of its underlying causes (Benford & Snow, 2000). Closely related to it is *prognostic framing*, which concerns the elaboration of potential solutions and intervention strategies (Snow & Benford, 1988).

Applied to the contemporary informational context, the concepts of *misinformation*, *disinformation*, and *infodemic* - which gained prominence during the COVID-19 pandemic and were subsequently consolidated in the literature (Calleja et al., 2021) - make it possible to interpret the communication crisis in diagnostic and prognostic terms: on the one hand, by identifying the problem in the excess and poor quality of circulating information within an ever-expanding information ecosystem; on the other, by proposing remedies based on the reliability of sources and the mitigation of information overload.

In recent years, the issue of information quality and verifiability has emerged as a major threat to public debate, social cohesion, and even democracy itself (Pira, 2023; Ferreira & Borges, 2020), influencing citizens' perceptions and the performance of key sectors such as healthcare (Di Falco et al., 2025*)* and the economy. False or unverified information, often presented in the style of traditional journalism and deliberately designed to deceive, spreads rapidly through social media, reaching millions of users and undermining informed decision-making (Figueira & Oliveira, 2017; Aldwairi & Alwahedi, 2018). News consumption through video-based platforms such as YouTube - second only to Facebook in audience reach - further amplifies this phenomenon, particularly in a context where increasingly sophisticated technologies enable the realistic manipulation of images and videos (Anderson, 2018).

Today, the development of artificial intelligence has fostered new forms of disinformation through the creation of *deepfakes*, hyper-realistic audiovisual content generated by substituting a person's face or voice using neural networks (Maras & Alexandrou, 2019). This technology, now accessible to anyone with a computer, allows for the production of materials almost indistinguishable from reality, with potentially devastating implications (Fletcher, 2018; Hasan & Salah, 2019). Such processes severely challenge the Public Administration's capacity to preserve credibility, legitimize decisions, and maintain citizens' trust. They exemplify what many scholars describe as the *post-truth era*, in which digital disinformation and *information warfare* campaigns - often driven by malicious actors - become systematic instruments of opinion manipulation with direct repercussions on democratic institutions (Zannettou et al., 2019).

Against this backdrop, the purpose of this paper is to theoretically explore the epistemology of *misinformation*, *disinformation*, and *infodemic* - phenomena often examined separately but which, in the current context, converge in redefining the production and circulation of public information. Despite growing scholarly attention, the literature has largely neglected to address the dual role of Public Administration - both as a reactive actor, engaged in regulating and countering false information, and as a proactive actor, oriented toward building digital trust and fostering transparent institutional communication.

Adopting the interpretative categories of *diagnostic* and *prognostic framing*, this article aims to: (i) conceptualize *misinformation*, *disinformation*, and *infodemic* as interconnected dimensions of a complex systemic problem rooted in hyperconnectivity and information excess; (ii) analyze the forms, technologies, and regulatory frameworks shaping their diffusion; (iii) identify and discuss possible institutional strategies aimed at strengthening the communicative resilience of Public Administration.

Misinformation and Disinformation: Definitions, Nature and Implications

The definitions of information proposed by Shannon and Luhmann offer two complementary perspectives: on the one hand, information as a reduction of uncertainty (Shannon, 2001); on the other, information as a "*a difference that generates meaning or change*" (Luhmann, 1996). Both highlight that information is not a neutral element but a process that guides choices and structures social relations. In this sense, information represents one of the fundamental infrastructures of contemporary society: it sustains decision-making processes, shapes behaviors, and regulates interactions with Public Administration, either strengthening or weakening citizens' trust in institutions.

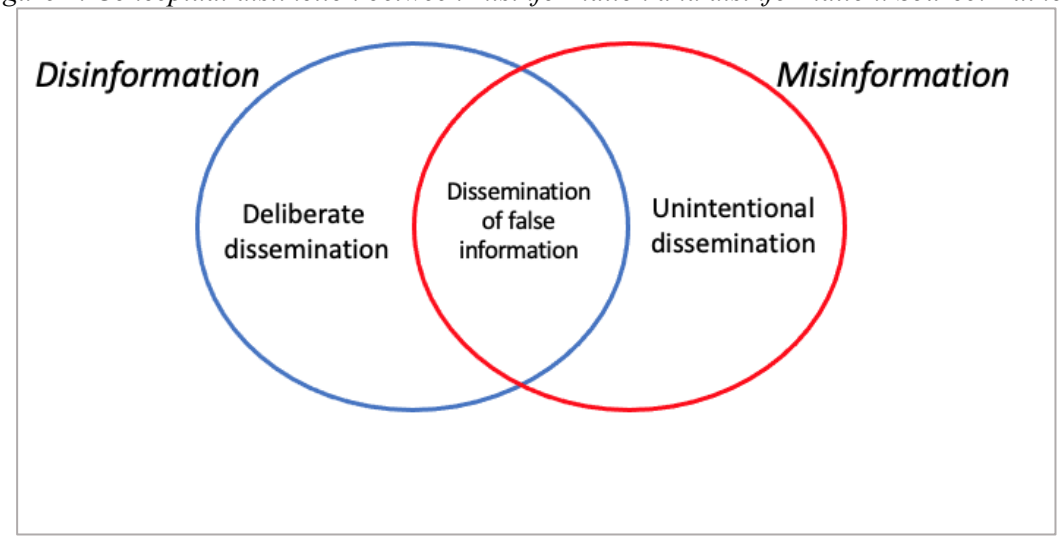
With the rise of the digital ecosystem, characterized by a continuous and pervasive flow of content, this centrality has been accompanied by new vulnerabilities that amplify the likelihood of encountering false, distorted, or manipulated information. It is precisely in this context that the need arises to distinguish between *misinformation* and *disinformation*, two categories that allow for a more precise qualification of the nature and implications of false information. As the digital environment has expanded, information has become not only more accessible but also more exposed to distortion and loss of reliability. A crucial aspect concerns the circulation of inaccurate, incomplete, or unverified content, which fuels confusion and undermines the quality of public discourse. However, not all incorrect information originates from the same causes or serves the same purposes. Some forms result from unintentional errors or non-rigorous communication processes, while others are the product of deliberate manipulation strategies. To differentiate between these dynamics, the literature has developed the categories of *misinformation* and *disinformation*, which are often intertwined in their effects but fundamentally distinct in nature and implications.

University of Messina - Journal homepage: https://cab.unime.it/journals/index.php/ASMC/
Addiction & Social Media Communication, 2025, Vol.2, No.2, pag: 3-20

Disinformation differs from *misinformation* in its intentionality. Unlike *misinformation*, which may stem from error or negligence, *disinformation* is always deliberate and goal-oriented, serving specific political, economic, or social purposes. While misinformation arises from mistakes or the unintentional sharing of inaccurate information, disinformation is consciously constructed to influence opinions, manipulate behavior, or weaken institutions, as illustrated in *Figure 1*. According to Obushna et al. (2023), *disinformation* can be defined as the dissemination of false or misleading information, deliberately created and distributed to deceive the public and cause harm to society, public administration, or individuals.

This definition clearly identifies the key element distinguishing *disinformation* from *misinformation*: it is not a random error or oversight but an intentional process aimed at manipulating public perception and producing tangible social, political, and economic effects. In recent years, even *misinformation*, despite lacking deliberate intent, has shown the capacity to generate destabilizing effects at multiple levels, with consequences comparable to those of *disinformation*. Beyond compromising journalistic integrity, it has produced significant impacts in economic, political, and democratic domains (Pira, 2023; Roberts, 2017; Bastos & Mercea, 2019; Lawrence & Silverman, 2016; Petratos, 2021), extending its influence into public health and the daily lives of citizens (Calleya et al., 2021; Bowen, 2025; Zlatanovic & Powell, 2024).

Figure 1. Conceptual distinction between misinformation and disinformation. Source: Authors.



In the case of *disinformation*, scholars have identified several recurring characteristics of such content: relevance to the target audience, artificial construction of the message, intentional dissemination, timing, apparent credibility, and focus on specific targets (Obushna et al., 2023).

This enumeration highlights the strategic nature of *disinformation*: it does not merely consist in the creation of false content but in the design of narratives that appear plausible, resonate with individuals' informational needs, and exploit the most favorable moments for diffusion. In this sense, the danger of *disinformation* lies not only in the falsity of its content but also in its ability to exploit cognitive vulnerabilities and technological mechanisms that amplify its reach. As Lazer et al. (2018) observe, *disinformation* has deep historical roots but now takes radically new forms due to the channels through which it circulates. The advent of the Internet, followed by social media, has transformed both the scale and the speed at which false or inaccurate content spreads, generating unprecedented effects on the quality of information and the functioning of contemporary societies.

From an academic perspective, research on this topic has produced in recent years a growing body of studies addressing the phenomenon from multiple angles. Some have focused on analyzing the social and informational dynamics that characterize the spread of *disinformation* and its consequences (Agarwal et al., 2020; Bauman, 2002, 2006, 2013; Bradshaw & Howard, 2018; Lazer et al., 2018; Morozov, 2011; Pariser, 2011; Quattrociocchi & Vicini, 2017; Rashidian et al., 2018; Zannettou et al., 2019), while others have developed methodological and technological approaches for the automatic detection of online fake news sources (Shu et al., 2017; Pérez-Rosas et al., 2018; Zhang & Ghorbani, 2020; Zhou et al., 2019).

This dual perspective - interpretive and technological - demonstrates that *misinformation* and *disinformation* are not merely communicative issues but complex, interdisciplinary phenomena that demand integrated responses combining critical analysis with technical innovation.

This contribution seeks to further examine the impact of *misinformation* and *disinformation* on Public Administration and the construction of institutional trust. These phenomena undermine the credibility of institutions, complicate policy implementation, and may compromise democratic cohesion by exposing citizens to manipulative messages that weaken the effectiveness of public action.

Unpacking Misinformation and Disinformation: Forms, Patterns and Effects

Although the distinction between misinformation and disinformation is conceptually well established, in practice the boundary between the two often appears blurred. It is not always straightforward to determine whether a given piece of content has been disseminated with the intention to deceive or rather as the result of misunderstanding, inaccurate communication, or limited contextualization. Forms of expression such as satire or parody, for instance, may be interpreted literally by part of the audience and thus unintentionally contribute to misinformation, while similar communicative techniques can also be deliberately employed to manipulate public opinion, discredit institutions, or harm specific actors, thereby constituting disinformation.

This ambiguity highlights that the nature and impact of information depend not only on the content itself, but also on its context of circulation, the social dynamics surrounding its diffusion, and, above all, the intentionality of the actors involved. On this basis, the literature has identified several recurrent forms through which these dynamics manifest themselves, as summarized in Table 1.

Fake news represents one of the most visible and widely studied forms of disinformation. They consist of intentionally false and verifiable articles produced with the aim of misleading audiences. Zhang and Ghorbani (2020) adopt a broader definition, encompassing artificially constructed narratives disseminated - primarily through online channels - for political or economic purposes (Gray, 2017; Britt et al., 2019). The systematic use of fake news during the 2016 U.S. presidential elections demonstrated their capacity to influence public opinion and electoral processes (Meel & Vishwakarma, 2021). Importantly, fake news do not always rely on entirely fabricated content, but often build upon genuine information that is selectively manipulated or decontextualized, making detection more difficult. In this sense, disinformation has become a structural component of contemporary communicative processes, driven by platform logics and data exploitation (Pira, 2023).

Alongside fake news, rumours play a significant role in the disinformation ecosystem. Rumours are characterized by ambiguous or unverified content circulating in the absence of supporting evidence (Walker & Blaine, 1991). The affordances of social media have considerably amplified their diffusion, facilitating the spread of narratives lacking factual grounding. As shown by Zubiaga et al. (2017), similar dynamics have persisted over time, repeatedly influencing public debate and contributing to collective uncertainty.

Another relevant category is that of hoaxes, namely fabricated stories that may carry humorous, satirical, or malicious intent. Hoaxes often intersect with rumours or urban legends and spread as if they were verified information. Their effectiveness lies in their ability to exploit social credibility and audience curiosity (Kumar, West, & Leskovec, 2016), allowing them to circulate widely before being corrected.

Disinformation also includes biased or one-sided news, which are not necessarily false but are constructed through selective framing and partial representation of facts. In political contexts, this phenomenon is reflected in hyperpartisan news, characterized by explicit ideological alignment or support for specific actors. Such content contributes significantly to the polarization of public debate and the erosion of deliberative spaces (Potthast et al., 2017).

Finally, among the most recent and problematic forms of disinformation are deepfakes, namely synthetic audiovisual content generated through artificial intelligence techniques.

By employing neural networks and machine learning systems, deepfakes enable the creation of highly realistic images, videos, or audio recordings that are increasingly difficult to distinguish from authentic material (Chawla, 2019; Xu et al., 2022). Their diffusion poses particularly serious risks, as they undermine the very possibility of reliably distinguishing between authentic and manipulated content (Guo et al., 2020). Taken together, these forms of disinformation outline a complex constellation of practices that exploit cognitive vulnerabilities, social dynamics, and advanced digital technologies. Rather than representing isolated phenomena, they generate differentiated challenges for public institutions, complicating citizens' ability to navigate an overloaded informational environment and contributing to the erosion of trust in institutions and public discourse.

Table 1. Forms of disinformation and communicative effects. Source: Authors.

Form	Description	Main characteristics	Typical examples
Fake news	Intentionally false and verifiable articles or news items	Deliberate deception, plausibility, rapid online dissemination	2016 U.S. elections, fabricated news about vaccines
Rumours	Unverified beliefs or claims of ambiguous truth	Lack of evidence, viral spread on social media	Alleged miracle cures for COVID-19
Hoaxes	Fabricated stories often linked to urban legends	Humorous or malicious intent, appearance of truth	False announcements of celebrity deaths
Biased / one-sided news	True content constructed with strong partiality	Selective manipulation of data, polarization	*Hyperpartisan* news supporting a party or leader
Deepfakes	AI-generated digital content manipulating voice, face, or images	Extreme realism, ease of production, detection dif	Fake videos of politicians making statements they never actually made

Infodemic: From Information Overload to Institutional Vulnerability

While the distinction between *misinformation* and *disinformation* helps to clarify the nature and intentions underlying false or misleading content, it is not sufficient to explain the complexity of the contemporary informational environment that public administrations must also manage. Even accurate information, when disseminated excessively, without context, or in a disorganized manner, can generate confusion and weaken citizens' critical capacity.

Within this perspective, the concept of *infodemic* emerges - a phenomenon that does not concern only the falsity of content but rather the uncontrolled proliferation of information - whether true, partial, or false - which makes it increasingly difficult to distinguish reliable sources from manipulative ones.

Despite the efforts of the scientific and policy communities, *disinformation* remains a difficult concept to classify and standardize. The various taxonomies rely on different criteria - from intent to factuality, authenticity, and falsifiability - yet struggle to converge into a shared conceptual framework (Tandoc et al., 2020; Freelon & Wells, 2020). This fragmentation risks making the term "disinformation" a generic and poorly operational category, overlooking the fact that the threat associated with certain statements depends not only on their degree of accuracy but also on the impact they may have on society and institutions.

The notion of *infodemic* allows this conceptual impasse to be overcome, as it provides a broader framework within which *disinformation* can be situated, along with the possible actions that public administrations may undertake. It highlights not only the communicative nature of content but also its social, political, and institutional consequences.

The *infodemic*, understood as an overabundance of not always reliable information, is closely linked to the spread of *fake news* and to the limited ability of a significant share of the population to critically assess sources. In Italy, according to the *Eurobarometer* report[1] (2025), only 46% of people possess basic digital skills, compared with a European average of 54% - a circumstance that increases vulnerability to false or manipulative content. Digital platform algorithms, as noted by Pariser (2011), tend to construct *filter bubbles* that reinforce pre-existing biases and opinions, reducing exposure to different perspectives and fueling polarization. This mechanism, often intensified by so-called *echo chambers*, undermines the formation of a high-quality public sphere and risks eroding trust in institutions and science.

Regulating Disinformation: Between Freedom of Speech and Institutional Accountability

In light of the analytical framework developed in the previous sections**,** understanding the dynamics of misinformation, disinformation, and infodemic is not only analytically relevant but also essential for assessing the regulatory and institutional responses developed to address these challenges.

The regulation of *disinformation* raises complex questions, particularly concerning the distinction between *misinformation* - the unintentional dissemination of false news - and *disinformation*, characterized by deliberate manipulative intent. This difference is not always reflected in legal systems. Some jurisdictions, such as Tunisia's *Decree-Law No. 54/2022* or the provisions introduced in Russia between 2019 and 2020, criminalize the dissemination of "false information" in general terms, without requiring proof of intent, thereby risking sanctions against citizens acting in good faith or independent journalists.

[1] European Commission. (2025). *Eurobarometer 2025*. Directorate-General for Communication. https://europa.eu/eurobarometer

In Italy, the issue is addressed in a more traditional manner, balancing Article 21 of the Constitution (freedom of expression) with criminal provisions such as Article 656 of the Penal Code, which punishes the dissemination of false or tendentious news likely to disturb public order. This demonstrates that the problem of *fake news* did not originate in the digital era, but has been exacerbated by the speed and reach of online circulation. However, Italian regulation remains fragmented and reactive - focused more on *ex post* repression than on systemic prevention.

At the European level, by contrast, a more systemic and multi-level approach has emerged. The *Digital Services Act* and the *Code of Practice on Disinformation* (2022) introduce obligations for digital platforms: greater transparency, mechanisms for demonetizing misleading content, cooperation with independent fact-checkers, and access to data for research purposes. Complementing these measures is the establishment of the *European Digital Media Observatory* (EDMO), which coordinates national hubs engaged in research, fact-checking, and media literacy initiatives.

These developments reflect a growing awareness: indiscriminately punishing *misinformation* and *disinformation* can generate unintended consequences, such as disproportionate restrictions on freedom of expression or risks of political censorship. The true regulatory challenge, therefore, is not merely to repress false content but to govern the systemic dynamics of the information ecosystem -by holding platforms accountable, strengthening democratic resilience, and, above all, building trust between citizens and institutions.

Within this framework, public administration plays a crucial dual role: as a *regulatory actor* and as a *primary source of credible information*. However, managing *disinformation* cannot be seen as an exclusively institutional responsibility. The informational resilience of a country also depends on civic competence and participation: citizens, beyond being the targets of counter-disinformation policies, become co-protagonists through informed behaviors, verification capabilities, and collaboration with institutions in fostering *digital trust*.

The Italian Case: Institutionalizing the Social Media & Digital Manager in Public Administration

In recent years, alongside the broader debate on the quality of information in the digital society, the issue of *communicative quality* within public institutions has emerged with increasing relevance -understood as the public administration's ability to produce, manage, and disseminate reliable information consistent with its objectives of transparency and accountability.

Within this framework, the growing regulatory attention toward the communicative dimension of governance has highlighted the need for institutional instruments capable of integrating technological innovation, informational responsibility, and public trust.

It is precisely in this direction that the introduction, within the Italian context, of the *Social Media & Digital Manager* (SMDM) can be situated. This role represents an attempt to translate into practice a new vision of communication as a strategic function of public administration.

The measure was formally introduced by *Decree-Law No. 25 of 14 March 2025*, later converted into *Law No. 69 of 9 May 2025*, titled "Urgent provisions on recruitment and functionality of public administrations." Article 4, paragraph 9-*novies*, authorizes administrations to appoint, either from existing staff or through new recruitment, a *Social Media & Digital Manager* responsible for developing communication strategies tailored to social media, managing institutional digital platforms, promoting informed citizen participation, and ensuring the qualitative verification of released information.

Although still in the implementation phase, this provision marks a significant evolution: it acknowledges that the prevention and mitigation of *misinformation*, *disinformation*, and *infodemic* phenomena cannot rely solely on punitive or technological measures, but require specialized professional competencies devoted to the design and management of public information.

The experience gained during the COVID-19 pandemic clearly demonstrated how the lack of coordinated communication within public administrations can amplify citizens' exposure to misleading content, generating confusion and distrust. During that phase, overlapping institutional messages and the absence of structured communication strategies revealed the urgency of professional profiles capable of ensuring clarity, timeliness, and verifiability of public information.

The establishment of the SMDM can thus be interpreted as a systemic response to these criticalities: a professional figure entrusted with a *cognitive and reputational stewardship* function, capable of monitoring and mitigating the spread of distorted content while strengthening the legitimacy of institutional discourse in the digital context.

From an applied perspective, the effectiveness of the Social Media & Digital Manager relies on a set of specialized competencies that reflect the informational challenges outlined in the previous sections. Beyond technical skills related to social media management, the role requires advanced capabilities in institutional digital communication, content verification, and source validation, as well as a solid understanding of platform logics and data-driven information flows (Mergel, 2017). These competencies are essential for addressing misinformation through timely clarification and transparent communication, countering disinformation via monitoring and reputational safeguarding, and managing infodemic dynamics through message prioritization and cross-institutional coordination. In this sense, the SMDM operates at the intersection of communication, governance, and cognitive responsibility, translating diagnostic insights into prognostic action. The role thus embodies an applied form of cognitive governance, in which professional skills are mobilized not only to disseminate information, but to preserve informational quality, institutional credibility, and public trust in a complex and saturated digital environment.

The institutionalization of this role is part of a broader process of progressive digitalization of the public sector, yet one still characterized by structural vulnerabilities. According to *ISTAT*[2] (2024), 86.2% of Italian households have Internet access, but persistent generational and territorial inequalities affect the ability to access, understand, and critically assess information, thereby increasing vulnerability to disinformation circuits. At the same time, public administration ICT expenditure, estimated by *AgID*[3] at around €3.8 billion in 2022 and projected to exceed €5 billion by 2025, signals a significant infrastructural investment that must be matched by a corresponding enhancement of internal communication and digital skills.

From a comparative perspective, Italy ranks slightly below the OECD[4] average in the *Digital Government Index* (0.58 versus 0.61), but shows progress in the "Digital by Design" dimension - an indication of increasing integration of digital innovation into public policy and service design.

Within this trajectory, the *Social Media & Digital Manager* can be interpreted as an operational cornerstone of the cognitive governance of public administration, oriented toward building *digital public value* based on transparency, inclusion, and reliability.

[2] ISTAT. (2024). *Citizens and ICT – 2024*. Italian National Institute of Statistics. https://www.istat.it/comunicato-stampa/cittadini-e-ict-anno-2024/
[3] AgID. (2025). *ICT expenditure in public administration: AgID publishes the 2025 report*. Agenzia per l'Italia Digitale. https://www.agid.gov.it/it/notizie/spesa-ict-nella-pa-pubblicato-il-nuovo-report-di-agid
[4] OECD. (2020). *The OECD Digital Government Policy Framework: Six dimensions of a digital government* (OECD Public Governance Policy Papers, No. 2). OECD Publishing. https://www.oecd.org/en/publications/the-oecd-digital-government-policy-framework_f64fed2a-en.html

Discussion and Conclusion

The originality of this contribution lies in framing public administration not merely as a regulatory authority responding to disinformation, but as an active cognitive agent capable of structuring the informational environment. By integrating diagnostic and prognostic framing with institutional communication and governance practices, the article offers a novel analytical lens for understanding how public administrations can proactively enhance informational quality and democratic trust.

The analysis conducted shows that *misinformation, disinformation, and infodemic* are not merely communicative phenomena, but structural components of the contemporary information ecosystem. Their pervasiveness - amplified by the speed, interconnection, and fragmentation of the digital environment - raises crucial questions about the ability of public institutions to preserve the quality of information and, consequently, collective trust. From this perspective, these phenomena should not be understood as isolated categories, but rather as interconnected dimensions of a systemic problem operating at the cognitive, social, and institutional levels. For the purpose of conceptual synthesis, *Table 2* summarizes the main distinctive features of misinformation, disinformation, and infodemic as they emerged from the theoretical analysis developed in this contribution, clarifying the different logics through which they affect the information ecosystem and contribute to the communicative vulnerability of public institutions.

Read through a diagnostic–prognostic framing, these distinctions provide an analytical basis for guiding differentiated institutional strategies, allowing Public Administration to calibrate its communicative, organizational, and regulatory responses according to the specific nature of the informational challenge.

Table 2. Conceptual distinctions between misinformation, disinformation, and infodemic. Source: Authors.

Concept	Definition	Key distinguishing feature
Misinformation	The circulation of false, inaccurate, or unverified information disseminated without manipulative intent, often resulting from error, misunderstanding, or non-rigorous communication processes. Despite the absence of intentionality, misinformation can produce destabilizing effects on public debate, collective decision-making, and institutional trust.	Absence of manipulative intent
Disinformation	The intentional and strategic production and dissemination of false or misleading content designed to appear credible, exploit cognitive and technological vulnerabilities, and influence opinions, behaviors, or decision-making processes, with significant political, social, or institutional effects.	Intentionality and manipulative purpose
Infodemic	The uncontrolled overabundance of information - whether true, partial, or false - that, regardless of its accuracy, generates cognitive confusion, reduces citizens' critical capacity, and makes it difficult to distinguish reliable sources from manipulative ones, thereby increasing institutional vulnerability.	Information overload and systemic disorder

On this basis, public administration no longer emerges as a merely regulatory actor, but as a cognitive agent and guarantor of truthfulness. However, it must operate in a dual capacity: on one hand, as a safeguard against disinformation and informational manipulation; on the other, as a promoter of a model of public communication based on accuracy, coherence, and transparency - one capable of preventing the very formation of *dis-* and *misinformative* circuits. In this sense, the Public Administration not only combats disinformation but contributes to immunizing its own communicative ecosystem, ensuring quality and trust in the institutional production of information.

The theoretical discussion highlights that disinformative phenomena cannot be addressed solely through repressive or technological means. They require an epistemological rethinking of the relationship between information, trust, and governance. As Luhmann (1996) reminds us, trust is a mechanism for reducing communicative complexity and, in the digital context, constitutes an essential democratic resource - a prerequisite for citizens to navigate consciously within an ever-changing flow of information. Building digital trust thus implies defining multilayered strategies that integrate normative, technological, and cultural dimensions, positioning the Public Administration at the center of this balance.

At the institutional level, strengthening the Public Administration's communication channels as primary sources of certified information becomes a priority. Transparency, timeliness, and message consistency are not merely organizational requirements but enabling conditions of public trust. From this perspective, public communication must evolve from an accessory function to a *cognitive infrastructure of democracy*, capable of connecting citizens, media, and institutions within a circuit of reciprocal legitimization. As Pira (2023) notes, the quality of institutional communication directly affects the ability to prevent disinformation by reducing spaces of ambiguity and manipulation.

The introduction of the *Social Media & Digital Manager* (SMDM) within the Italian context represents a significant step in this direction. This figure - established by *Decree-Law No. 25 of 14 March 2025*, converted into *Law No. 69 of 9 May 2025* - embodies an operational model of cognitive governance: an internal actor within the Public Administration capable of combining communicative, digital, and relational competencies to ensure the quality, coherence, and timeliness of information disseminated through institutional channels. The SMDM serves as both a reputational and cognitive safeguard, mitigating the public ecosystem's vulnerability to disinformative flows while reinforcing the link between transparency, participation, and trust. This approach aligns with the European paradigm of *digital accountability*, which promotes communicative responsibility as a form of democratic guarantee.

Alongside institutional strengthening, the role of media and digital literacy emerges with equal importance. Combating disinformation cannot be delegated solely to platforms or regulatory authorities - it requires the active involvement of citizens as *co-producers of public truth*. From this perspective, promoting critical skills,

assessing source reliability, and using digital tools consciously are essential dimensions of informational citizenship. Literacy should thus be understood as a structural policy of *cognitive empowerment*, an integral part of public communication strategies and educational policies. An informed and competent citizenry represents the necessary foundation for democratic resilience.

Another key area of intervention concerns interinstitutional and public–private cooperation. Digital platforms, as infrastructures of contemporary communication, must be included in *co-regulation* mechanisms based on algorithmic transparency, data access, and shared responsibility. At the same time, collaboration with universities, research centers, and independent fact-checking agencies can contribute to building a national system of information monitoring and verification that combines scientific rigor with operational timeliness. Within this framework, the Public Administration is not merely a recipient of technological solutions but a promoter of *participatory information governance*, founded on cooperation among public, private, and civic actors.

The technological dimension remains a fundamental strategic lever. The use of *artificial intelligence*-based tools for monitoring information flows and detecting manipulated content can enhance institutional responsiveness. However, such tools must adhere to principles of transparency and *algorithmic accountability*, avoiding technocratic excesses or risks of informational surveillance. Technology can support - but not replace - critical judgment and human responsibility in managing public information.

Similarly, the communicative responsibility of the Public Administration is not limited to monitoring external information flows but extends to the design and quality of its own messages. Institutional communication that is free from *disinformation*, *misinformation* or *infodemic* distortions represents the first instrument of prevention and trust-building. The Public Administration must therefore act simultaneously as both regulator and model, demonstrating through its own communicative conduct the tangible possibility of credible, verifiable, and inclusive public information.

In conclusion, the fight against *misinformation*, *disinformation*, and *infodemic* should not be conceived as a set of emergency interventions but as a systemic process aimed at strengthening the cognitive capacity of democracy. Public administration is called to play a dual and integrated role: as guarantor of informational quality and as promoter of a communicative environment rooted in transparency, coherence, and truthfulness. Only a Public Administration capable of combining institutional rigor, digital competence, and communicative responsibility can act as a proactive actor in building digital trust. In this perspective, *public truth* is no longer a fixed asset to be safeguarded but a value to be collectively generated - through cooperation among institutions, citizens, and technologies. The construction of digital trust thus becomes not only a condition for the quality of public discourse but a new dimension of *public value*, capable of consolidating democratic legitimacy and the informational resilience of contemporary society.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article, or declared.

Funding

The author(s) received/no financial support for the research, authorship, and/or publication of this article.

References

1. Agarwal, P., Joglekar, S., Papadopoulos, P., Sastry, N., & Kourtellis, N. (2020). Stop tracking me bro! Differential tracking of user demographics on hyper-partisan websites. *Proceedings of the Web Conference 2020 (WWW '20)*, 1479–1490. ACM.
2. Aldwairi, M., & Alwahedi, A. (2018). Detecting fake news in social media networks. *Procedia Computer Science, 141*, 215–222. https://doi.org/10.1016/j.procs.2018.10.171
3. Anderson, K. E. (2018). Getting acquainted with social networks and apps: Combating fake news on social media. *Library Hi Tech News, 35*(3), 1–6.
4. Bastos, M. T., & Mercea, D. (2019). The Brexit botnet and user-generated hyperpartisan news. *Social Science Computer Review, 37*(1), 38–54. https://doi.org/10.1177/0894439317734157
5. Bauman, Z. (2002). *Modernità liquida*. Laterza.
6. Bauman, Z. (2006). *Modus vivendi*. Laterza.
7. Bauman, Z. (2013). *Liquid surveillance: A conversation with David Lyon*. Polity Press.
8. Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Annual Review of Sociology, 26*, 611–639.
9. Bowen, F. R. (2025). Misinformation and disinformation are harmful to your health. *Journal of Pediatric Health Care, 39*(5), 701–702.
10. Bradshaw, S., & Howard, P. N. (2018). *Challenging truth and trust: A global inventory of organized social media manipulation*. Oxford Internet Institute.
11. Britt, M. A., Rouet, J.-F., Blaum, D., & Millis, K. (2019). A reasoned approach to dealing with fake news. *Policy Insights from the Behavioral and Brain Sciences, 6*(1), 94–101. https://doi.org/10.1177/2372732218814855
12. Calleja, N., AbdAllah, A., Abad, N., Ahmed, N., Albarracin, D., Altieri, E., Purnat, T. D. (2021). A public health research agenda for managing infodemics: Methods and results of the First WHO Infodemiology Conference. *JMIR Infodemiology, 1*(1), e30979. https://doi.org/10.2196/30979
13. Chawla, R. (2019). Deepfakes: How a pervert shook the world. *International Journal of Advance Research and Development, 4*(6), 4–8.
14. Di Falco, C., Noto, G., & Barresi, G. (2025). Dalla misurazione dell'outcome a quella dell'impact: La sentiment analysis a supporto della valutazione della performance delle aziende sanitarie pubbliche. *Management Control*, (2).
15. Ferreira, G. B., & Borges, S. (2020). Media and misinformation in times of COVID-19: How people informed themselves in the days following the Portuguese declaration of the state of emergency. *Journalism and Media, 1*(1), 108–121.
16. Figueira, A., & Oliveira, L. (2017). The current state of fake news: Challenges and opportunities. *Procedia Computer Science, 121*, 817–825. https://doi.org/10.1016/j.procs.2017.11.106

17. Fletcher, J. (2018). Deepfakes, artificial intelligence, and some kind of dystopia: The new faces of online post-fact performance. *Theatre Journal, 70*(4), 455–471. https://doi.org/10.1353/tj.2018.0097
18. Freelon, D., & Wells, C. (2020). Disinformation as political communication. *Political Communication, 37*(2), 145–156.
19. Gray, R. (2017). Lies, propaganda and fake news: A challenge for our age. *BBC Future*. https://www.bbc.com/future/article/20170301-lies-propaganda-and-fake-news-a-grand-challenge-of-our-age
20. Guo, B., Ding, Y., & Yao, L. (2020). The future of false information detection on social media: New perspectives and trends. *ACM Computing Surveys, 53*(4), 1–36. https://doi.org/10.1145/3393880
21. Hasan, H. R., & Salah, K. (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access, 7*, 41596–41606. https://doi.org/10.1109/ACCESS.2019.2905689
22. Kumar, S., West, R., & Leskovec, J. (2016). Disinformation on the web: Impact, characteristics, and detection of Wikipedia hoaxes. *Proceedings of the 25th International Conference on World Wide Web (WWW '16)*, 591–602.
23. Lawrence, A., & Silverman, C. (2016). How teens in the Balkans are duping Trump supporters with fake news. *BuzzFeed News*.https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo
24. Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., & Pennycook, G. (2018). The science of fake news. *Science, 359*(6380), 1094–1096. https://doi.org/10.1126/science.aao2998
25. Luhmann, N. (1996). *Modern society shocked by its risks*. Polity Press.
26. Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *International Journal of Evidence & Proof, 23*(3), 255–262. https://doi.org/10.1177/1365712718807226
27. Meel, P., & Vishwakarma, D. K. (2021). Machine learned classifiers for trustworthiness assessment of web information contents. *Proceedings of the International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 29–35. IEEE.
28. Mergel, I. (2017). Social media communication modes in government. In J. R. Gil-Garcia, T. A. Pardo, & T. Nam (Eds.), *Routledge handbook on information technology in government* (pp. 168–179). Routledge.
29. Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. PublicAffairs.
30. Obushna, N., Korchak, N., Evsyukova, O., Selivanov, S., & Larin, S. (2023). Mechanisms for preventing disinformation in public administration: Current issues. *Management Theory and Studies for Rural Business and Infrastructure Development, 45*(4), 467–476.
31. Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. Penguin.
32. Pérez-Rosas, V., Kleinberg, B., Lefevre, A., & Mihalcea, R. (2018). Automatic detection of fake news. *Proceedings of COLING 2018*, 3391–3401.

33. Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons, 64*(6), 763–774.
34. Pira, F. (2023). Disinformation as a problem for democracy: Profiling and risks of consensus manipulation. *Frontiers in Sociology, 8*, 1150753. https://doi.org/10.3389/fsoc.2023.1150753
35. Potthast, M., Kiesel, J., Reinartz, K., Bevendorff, J., & Stein, B. (2017). A stylometric inquiry into hyperpartisan and fake news. *arXiv preprint*, arXiv:1702.05638.
36. Quattrociocchi, W., & Vicini, A. (2017). *Misinformation: Guida alla società dell'informazione e della credulità*. FrancoAngeli.
37. Rashidian, N., Brown, P., Hansen, E., Bell, E., Albright, J., & Harstone, A. (2018). *The platform press: At the heart of journalism*. Tow Center for Digital Journalism.
38. Roberts, J. J. (2017). Hoax over 'dead' Ethereum founder spurs $4 billion wipe out. *Fortune*. https://fortune.com/2017/06/26/vitalik-death/
39. Shannon, C. E. (2001). A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review, 5*(1), 3–55.
40. Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake news detection on social media: A data mining perspective. *SIGKDD Explorations, 19*(1), 22–36. https://doi.org/10.1145/3137597.3137600
41. Snow, D. A., & Benford, R. D. (1988). Ideology, frame resonance, and participant mobilization. *International Social Movement Research, 1*, 197–218.
42. Tandoc, E. C., Lim, D., & Ling, R. (2020). Diffusion of disinformation: How social media users respond to fake news and why. *Journalism, 21*(3), 381–398.
43. Walker, C. J., & Blaine, B. (1991). The virulence of dread rumors: A field experiment. *Language & Communication, 11*(2), 291–297.
44. Xu, F. J., Wang, R., Huang, Y., et al. (2022). Countering malicious deepfakes: Survey, battleground, and horizon. *International Journal of Computer Vision*. https://doi.org/10.1007/s11263-022-01606-8
45. Zannettou, S., Sirivianos, M., Blackburn, J., & Kourtellis, N. (2019). The web of false information: Rumors, fake news, hoaxes, clickbait, and various other shenanigans. *Journal of Data and Information Quality, 11*(3), Article 10. https://doi.org/10.1145/3309699
46. Zhang, X., & Ghorbani, A. A. (2020). An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management, 57*(2), 102025. https://doi.org/10.1016/j.ipm.2019.03.004
47. Zhou, X., Zafarani, R., Shu, K., & Liu, H. (2019). Fake news: Fundamental theories, detection strategies and challenges. *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining (WSDM '19)*, 836–837.
48. Zlatanovic, P., & Powell, J. (2024). Medical disinformation is bad for your health. *European Journal of Vascular and Endovascular Surgery, 67*(5), 746.
49. Zubiaga, A., Liakata, M., & Procter, R. (2017). Exploiting context for rumour detection in social media. In *International Conference on Social Informatics* (pp. 109–123). Springer.