

Appendix H: The French counter-disinformation context

Terminology in institutional usage. In French public documents, “désinformation” commonly functions as an umbrella term. While scholarship distinguishes disinformation (false, deliberately harmful), misinformation (false, shared in good faith), and malinformation (accurate, weaponized to harm) (Wardle & Derakhshan, 2017), institutional texts routinely use “disinformation” for the whole spectrum of information manipulation (e.g., Assemblée nationale, 2025), and the European Commission’s Code of Practice on Disinformation, though formally defining disinformation narrowly, in practice covers phenomena from foreign interference to political propaganda (Darcy, 2026a, pp. 7–10).

Legal instruments. French law has never created a general offense of disinformation; it proceeds through scattered provisions sanctioning specific harmful uses of falsehood (Darcy, 2026a, ch. 5). The 1881 press law (Article 27) penalizes false news published in bad faith and liable to disturb public peace; the electoral code targets false electoral news and bans commercial advertising for propaganda purposes. The 2018 law against the manipulation of information added a fast-track judicial procedure (Article L. 163-2 of the electoral code) against manifestly false or misleading information disseminated massively and deliberately during electoral periods; the Constitutional Council upheld the procedure while narrowing its scope, and to our knowledge the procedure has been used only once (2019, rejected). The May 2024 law on securing and regulating the digital space (SREN law) repealed several provisions of the 2018 law and aligned French law with the European Union (EU) Digital Services Act (DSA), shifting the center of gravity of platform regulation to the European level.

Institutional apparatus. The national strategy against information manipulation, adopted in February 2026 under the Secrétariat général de la défense et de la sécurité nationale (SGDSN), after the present survey’s fieldwork was completed, organizes French action around four pillars: societal resilience; regulation of platforms and generative artificial intelligence (AI) services; operational capacity against foreign digital interference; and allied action for a free, open, and secure information space (SGDSN, 2026). VIGINUM (Vigilance et protection contre les ingérences numériques étrangères), a service created in 2021 and attached to the SGDSN, is mandated not to counter disinformation in general but to detect and characterize foreign digital interference: campaigns involving a foreign actor and the artificial, massive, and deliberate dissemination of manifestly inaccurate or misleading content liable to harm the fundamental interests of the nation. A February 2026 decree extended its analytical scope to search engines and online interfaces and added public-information missions. Without coercive powers, it publishes reports on characterized campaigns (e.g., “Portal Kombat,” “Matriochka”). The Foreign Ministry created a monitoring and strategic-communication sub-directorate in 2022 and launched “French Response” in September 2025, an offensive debunking account on X that combines fact-restoration with rapid, platform-native ripostes. An active fact-checking and media-literacy sector completes the landscape.

Independent regulators. The Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), the audiovisual and digital communication regulator, is the authority most directly concerned with disinformation: it supervises broadcasters, enforces platforms’ duty to cooperate against

information manipulation under the 2018 law, and acts as France's lead Digital Services Coordinator under the DSA. The Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), the telecommunications regulator, shapes the infrastructure of the information environment: it enforces net neutrality, regulates the distribution of the press (a pluralism issue) and, since the 2024 SREN law, oversees cloud services and data-intermediation providers, with a doctrine extending openness principles to devices, platforms, and generative AI. The Commission nationale de l'informatique et des libertés (CNIL), the data-protection authority, intervenes where disinformation meets personal data, notably political microtargeting and profiling. Executives of such independent authorities are part of the surveyed population (see Methods).

International dimension. France's response is embedded in EU platform governance (DSA, Code of Practice) and North Atlantic Treaty Organization (NATO) strategic-communication frameworks. VIGINUM cooperates most closely with its German and Swedish counterparts and the European External Action Service (EEAS) StratCom division, receives requests for advice from European and non-European states, and is developing a training academy on information-manipulation detection (Sénat, 2024; SGDSN, 2026). The framing that dominates French public administration (detecting and documenting attributable foreign operations rather than regulating disinformation in general) exemplifies the security-centered orientation discussed in the main text (Darcy, 2026a, pp. 103–104).

Information environment. According to the Reuters Institute's Digital News Report, trust in news is low (29%, against a 37% global average) and has not recovered, though France's relative position has risen as trust fell faster elsewhere (Antheaume, 2026). Interest in news is similarly low (36%), and about a third of the public (37%) avoids it. The market is strained: leading broadcasters and large publishers are cutting costs and freezing journalist recruitment as advertising falls, even as a subscriber-funded segment grows (Mediapart, Le Monde, Le Figaro). Some conservative media have become more overtly partisan than in the past (Antheaume, 2026). The March 2026 local elections were hit by a disinformation campaign using sites built to imitate local news outlets (Antheaume, 2026). Majorities believe owners (66%) and politicians (64%) shape coverage (Antheaume, 2026). Yet this low trust coexists with comparatively strong press freedom (France ranks 25th of 180 on the Reporters Without Borders index, score 76.68).

Institutional and political environment. Comparative research places institutional trust at the center of disinformation susceptibility (Ejaz et al., 2025; Humprecht et al., 2020), and in France trust runs low across institutions, politics, and everyday life. The political setting is unstable: five prime ministers have served in a single presidential term, and the far right and far left draw the youngest voters (Antheaume, 2026). Political trust keeps falling: in the 2026 Centre de recherches politiques de Sciences Po (CEVIPOF) barometer, trust in the President dropped to 18% (from 23% a year earlier), half of respondents (51%) see nothing to be proud of in the democratic system, more than in Italy (40%), Germany (34%), or the UK (32%), and the perception of politicians as corrupt is widespread (CEVIPOF, 2026). Perceived integrity has fallen in step: France's score on Transparency International's Corruption Perceptions Index dropped to 66 of 100 in 2025, its lowest under the current methodology, though France stays in the cleaner half of countries (Transparency International, 2026). The deficit is long-standing: for decades the French have trusted their fellow citizens, public authorities, and markets less than comparable democracies, a self-reinforcing "society of distrust" rooted in a statist, corporatist model (Algan & Cahuc, 2007). The French also underestimate how trustworthy others are and trust less than actual cooperation warrants (Darcy et al., 2026), and polarization in the National Assembly has risen sharply (Algan et al., 2025). Institutional, political, and interpersonal distrust thus converge on the very condition the literature places at the center of susceptibility, and that the practitioners surveyed weight comparatively lightly (Finding 2).