CHAPTER 2
LEGAL RELATIONS: FROM THEORY TO PRACTICE

State Regulation of Countering Disinformation in EU Member States: From Content Intervention to Systemic Risk Governance and Democratic Resilience

Boris Zarkov[1], Alla Dombrovska[2]
[1]*Ph.D. (National Security), Academy of National and Information Security, Plovdiv, Bulgaria*
[2]*Ph.D. (Law), Associate Professor, Assistant Professor of the Department of Legal Support of Economic Activity, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine, Researcher, Scientific Center of Innovative Research, Pussi, Estonia, ORCID: https://orcid.org/0000-0003-4610-8220*

Citation:
Zarkov, B., & Dombrovska, A. (2026). State Regulation of Countering Disinformation in EU Member States: From Content Intervention to Systemic Risk Governance and Democratic Resilience. *Public Administration and Law Review*, (3(27), 72–81. https://doi.org/10.36690/2674-5216-2026-3-72-81

Received: August 25, 2026
Approved: September 29, 2026
Published: September 30, 2026

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC 4.0) license

Abstract. *The spread of disinformation has transformed from a media-quality problem into a multidimensional challenge for democratic institutions, electoral integrity, national security, and public trust. In the European Union, public intervention has consequently moved beyond the direct regulation of false content toward a layered governance model combining platform accountability, electoral transparency, synthetic-content disclosure, media pluralism, fact-checking, strategic communication, and societal resilience. The study aims to identify the principal models of state regulation used to counter disinformation in EU Member States and to explain how national approaches interact with the common EU regulatory framework. The research applies comparative legal and institutional analysis to EU legislation, European Commission policy instruments, national laws, and official institutional documents. Five Member States were selected as contrasting cases: France, Sweden, Finland, Poland, and Estonia. The comparison focuses on legal intervention, platform governance, foreign information manipulation, public communication, fact-checking support, media literacy, and protection of fundamental rights. The analysis shows that the EU has developed a multi-layer system centred on the Digital Services Act, the Code of Conduct on Disinformation, the Political Advertising Regulation, Article 50 of the AI Act, the European Media Freedom Act, and the European Digital Media Observatory. National systems differ substantially. France combines electoral law with an operational foreign-interference capability through VIGINUM. Sweden institutionalises psychological defence against hostile information influence. Finland relies strongly on systematic media literacy and preventive resilience. Poland combines state communication, citizen reporting, and analytical monitoring through the Ministry of Digital Affairs and NASK. Estonia integrates strategic communication and information resilience into broader national-security and government-communication structures. Effective regulation of disinformation is increasingly based not on defining truth by law, but on regulating risk-producing systems, increasing transparency, detecting coordinated manipulation, and strengthening societal resilience. Future studies should evaluate enforcement outcomes under the DSA and AI Act, measure the effectiveness of national resilience models, and examine the use of generative AI in cross-border influence operations.*

Keywords: *disinformation; misinformation; European Union; Digital Services Act; information manipulation; media literacy; psychological defence; democratic resilience.*
JEL Classification: H11; H83; K23; D83
Formulas: 0; fig.: 1; tabl.: 2; bibl.: 23

Introduction. The expression "fake news" is widely used but analytically imprecise. European policy distinguishes misinformation, which may be false without harmful intent, from disinformation, which involves deliberately false or misleading information intended to cause harm or secure political, strategic, or economic advantage. Foreign information manipulation and interference additionally concerns coordinated influence by foreign or foreign-linked actors. These distinctions matter because democratic states cannot regulate every false statement without risking disproportionate restrictions on freedom of expression and media pluralism.

The European response has therefore moved from a narrow concern with false online content toward broader information-space governance. The central question is no longer only whether a statement is true, but how platforms amplify content, how political advertising is financed and targeted, how synthetic media are disclosed, how foreign influence is detected, and how citizens develop information resilience.

This shift is visible in the current EU framework. The Digital Services Act (DSA) imposes systemic-risk obligations on very large platforms and search engines. The 2022 Code of Practice on Disinformation was integrated into the DSA framework in 2025 as a Code of Conduct. Regulation (EU) 2024/900 regulates transparency and targeting of political advertising. Article 50 of the AI Act applies transparency duties to deepfakes and specified AI-generated public-interest content from August 2026. The European Media Freedom Act strengthens media pluralism and editorial independence, while EDMO supports fact-checking, research, and media literacy (European Commission, 2025a, 2026a).

The resulting system does not create a general EU prohibition of disinformation. Responsibility is distributed across platforms, public authorities, media, researchers, fact-checkers, and citizens, while Member States add responses shaped by national institutional and security contexts.

Literature Review. Academic literature increasingly treats disinformation as a governance problem rather than a discrete category of unlawful speech. The DSA regulates systemic risks linked to platform design, recommender systems, advertising, and dissemination dynamics rather than creating a general duty to remove lawful but misleading content. Husovec (2024) stresses that the Commission may require proportionate risk mitigation but cannot create new substantive categories of illegal speech through DSA enforcement.

Risk-based regulation also creates implementation challenges. Nannini et al. (2025) call for empirical evaluation of DSA effects through risk assessments, audits, transparency, data access, and platform governance. Gsenger (2026) shows that platform rules on disinformation remain heterogeneous, so EU obligations coexist with platform-specific definitions and moderation practices.

A second strand concerns co-regulation. The EU Code of Practice

began as a voluntary framework and, after its 2025 integration into the DSA system, became a benchmark for platform responsibility, transparency, and external scrutiny (Bayer, 2024; European Commission, 2025a).

A third strand addresses democratic rights. Disinformation may affect electoral participation and trust, while overly restrictive responses can themselves harm freedom of expression. EU regulation therefore increasingly favours transparency, procedural safeguards, independent oversight, and resilience over broad content bans.

Member States also differ in how they distribute responsibility between law, security agencies, public communication, education, civil society, and media institutions. Comparative analysis is therefore more informative than searching for a single model of an anti-fake-news law.

Aims. The aim of this study is to compare state approaches to countering disinformation in selected EU Member States and to explain their relationship with the common European regulatory framework. The study addresses three research questions: RQ1: Which regulatory instruments constitute the current EU framework for countering disinformation? RQ2: What institutional models are used by Member States to detect, mitigate, and build resilience against disinformation? RQ3: How can public authorities reduce information-manipulation risks without creating disproportionate restrictions on freedom of expression, media pluralism, and democratic participation?

Methodology. The study uses comparative legal and institutional analysis combined with an integrative review of academic and official sources from 2018 to September 2026. Particular attention is paid to the consolidation of the DSA framework, political-advertising rules, and the entry into application of AI Act transparency obligations.

The EU-level analysis is based on the DSA, Regulation (EU) 2024/900, the AI Act, the European Media Freedom Act, the Code of Conduct on Disinformation, DSA election guidelines, the European Democracy Shield, and EDMO materials. Academic literature is used to interpret legal boundaries, co-regulation, platform governance, and fundamental-rights implications.

Five Member States were selected through maximum variation: France for legal and operational intervention; Sweden for psychological defence; Finland for preventive media literacy; Poland for state communication and NASK-based monitoring; and Estonia for strategic communication embedded in security and crisis governance.

The comparison uses six dimensions: legal basis; principal institution; regulatory target; intervention mechanism; resilience instruments; and fundamental-rights safeguards. The purpose is to identify governance logics and areas of convergence rather than to rank countries.

Results. The comparative analysis identifies a multi-level architecture in which EU rules target platform systems, advertising, synthetic content,

and media conditions, while Member States address national vulnerabilities such as elections, foreign interference, strategic communication, and citizen resilience. Table 1 summarises the principal EU instruments.

Table 1. EU-Level Regulatory Instruments for Countering Disinformation

Instrument	Primary object	Main mechanism	Regulatory logic
Digital Services Act	Systemic risks on VLOPs/VLOSEs	Risk assessment, mitigation, audits, transparency, data access	Platform accountability
Code of Conduct on Disinformation	Platform and advertising practices	Co-regulatory commitments and reporting	Regulated co-governance
Political Advertising Regulation	Political advertising and targeting	Sponsor, funding and targeting transparency; consent rules	Electoral transparency
AI Act, Article 50	AI-generated and manipulated content	Machine-readable marking and disclosure of deepfakes / specified public-interest content	Synthetic-content transparency
European Media Freedom Act	Media independence and pluralism	Editorial safeguards, ownership transparency, source protection	Information-environment integrity
EDMO	Fact-checking, research and media literacy	Cross-border coordination and evidence infrastructure	Independent resilience capacity

Source: developed by the authors based on EU legislation and European Commission documents.

The DSA is the central platform-governance instrument. Articles 34 and 35 establish systemic-risk assessment and mitigation for VLOPs and VLOSEs. The 2024 election guidelines recommend election-specific measures, cooperation with authorities and civil society, safeguards related to generative AI, incident-response mechanisms, and post-election reviews (European Commission, 2024). The DSA therefore targets systemic risks rather than making disinformation generally illegal.

The Code of Conduct adds a co-regulatory layer. Its 2025 integration into the DSA framework made signatory commitments on advertising, manipulative behaviour, fact-checking, researcher access, and user empowerment relevant benchmarks for platform compliance (European Commission, 2025a).

Regulation (EU) 2024/900 adds an electoral-transparency regime requiring information on sponsors, funding, relevant elections, and targeting. Political-advertising targeting based on personal data is subject to explicit-consent requirements and restrictions on profiling with special-category data. The legal focus is therefore source and targeting transparency rather than truth adjudication.

Article 50 of the AI Act extends transparency to synthetic media. From 2 August 2026, relevant providers must support detection through machine-readable marking, while deployers must disclose deepfakes and specified AI-generated public-interest content where applicable (European Commission,

2026a, 2026b).

The European Media Freedom Act and EDMO address the broader information environment. The EMFA safeguards media pluralism, editorial independence, sources, and ownership transparency, while EDMO supports a cross-border ecosystem of fact-checkers, researchers, and media-literacy experts.

Table 2. Comparative Models of State Counter-Disinformation Policy in Selected EU Member States

Country	Institutional model	Principal target	Core instruments	Dominant logic
France	Legal + operational	Electoral manipulation; foreign interference	2018 law; VIGINUM; election protection mechanisms	Targeted intervention
Sweden	Psychological defence	Hostile foreign information influence	Psychological Defence Agency; preparedness; guidance	National resilience
Finland	Preventive media literacy	Population vulnerability to misleading information	National media education policy; cross-sector education	Cognitive resilience
Poland	Monitoring + public communication	False narratives and information incidents	Ministry of Digital Affairs; NASK/OAD; reporting; campaigns	Detection and public resilience
Estonia	Strategic communication	Misinformation and hostile information operations	Government Office coordination; crisis communication; security policy	Institutional trust and resilience

Source: developed by the authors based on national laws and official institutional documents.

France: Legal Intervention and Foreign-Interference Detection. France combines electoral law with an operational foreign-interference capability. Law No. 2018-1202 introduced electoral and platform-related provisions concerning information manipulation and cooperation duties for online platforms. The framework is tied to defined electoral contexts rather than a general prohibition of false statements.

VIGINUM, created in 2021 under the General Secretariat for Defence and National Security, detects and characterises foreign digital interference targeting public debate. Its mandate concerns coordinated foreign manipulation rather than ordinary misinformation. During the 2026 municipal elections it operated within a national election-protection mechanism and reported foreign digital-interference operations (VIGINUM, 2026).

Sweden: Psychological Defence as a State Capacity. Sweden institutionalises psychological defence through the Psychological Defence Agency, which coordinates public and societal preparedness, supports authorities and organisations, and strengthens population resilience. It identifies and analyses malign information influence directed at Sweden by antagonistic foreign powers (Psychological Defence Agency, n.d.).

The model targets societal capacity rather than individual false statements. Guidance focuses on recognising influence techniques, strategic communication, critical thinking, and institutional preparedness, treating information resilience as part of national security.

Finland: Media Literacy and Preventive Resilience. Finland represents a preventive model centred on media literacy. Its national media education policy promotes high-quality, comprehensive, and systematic media education across population groups through education, libraries, media, public administration, and civil society (National Audiovisual Institute, 2019).

The Finnish approach treats media literacy as long-term resilience. This is important because legal tools can reduce systemic risks but cannot prevent every misleading narrative from reaching citizens.

Poland: Monitoring, Reporting, and Strategic Communication. Poland combines strategic communication, public-awareness campaigns, citizen reporting, and analytical monitoring. The Ministry of Digital Affairs works with NASK on national campaigns and maintains a reporting mechanism for suspected disinformation (Ministry of Digital Affairs of Poland, 2026).

NASK's Disinformation Analysis Center identifies false narratives, publishes reports, handles citizen submissions, and cooperates with national and international partners. Government data published in 2026 reported more than 46,000 disinformation-related items submitted by NASK to social platforms during 2025, demonstrating the monitoring dimension of the Polish model.

Estonia: Strategic Communication and Information Resilience. Estonia integrates counter-disinformation into strategic communication, crisis preparedness, and security policy. The Government Office Strategy 2023-2026 assigns the Government Office responsibility for strategic communication and for strengthening society's ability to counter misinformation in everyday and crisis situations. The coalition agreement also commits the state to reducing disinformation and improving responses to hostile information operations (Government Office of Estonia, 2023; Government of Estonia, 2023).

The Estonian model emphasises timely and credible public communication rather than a specialised statutory definition of fake news, reflecting the view that information vacuums and low institutional trust create vulnerabilities exploitable by hostile actors.

The country-level analysis shows that national counter-disinformation systems do not operate independently from the EU regulatory framework. Instead, Member States complement common European rules with institutional mechanisms adapted to their own security environment, administrative traditions, media systems, and resilience priorities. Figure 1 synthesises this relationship by linking the principal EU regulatory

instruments with the five national governance models identified in the comparative analysis.

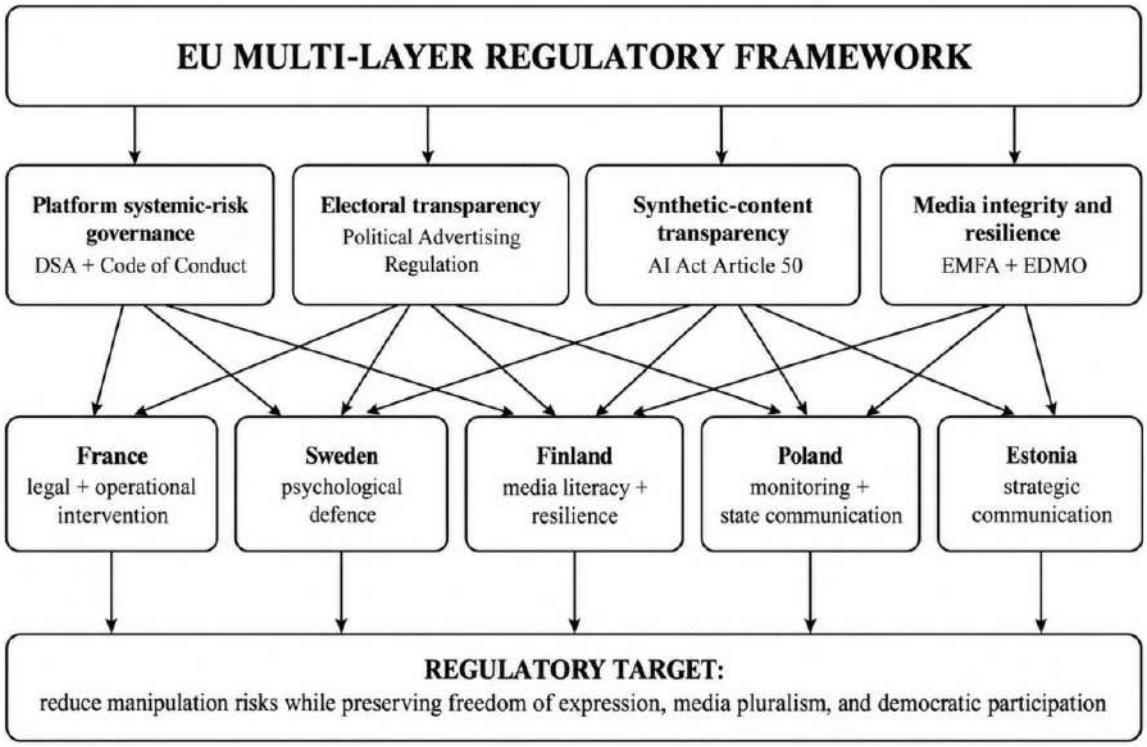


Figure 1. Multi-Layer Model of EU and Member-State Counter-Disinformation Governance

Source: developed by the authors based on the comparative analysis.

Figure 1 demonstrates that counter-disinformation governance in the EU is structured as a multi-layer system rather than as a single legal regime. EU-level instruments primarily establish common obligations concerning platform accountability, electoral transparency, synthetic-content disclosure, and media integrity, while national authorities operationalise these principles through legal intervention, psychological defence, media literacy, monitoring, and strategic communication. The resulting architecture therefore combines regulatory harmonisation at the European level with institutional differentiation at the national level.

Discussion. The results reveal four regulatory logics: systemic-risk governance under the DSA; transparency regulation for political advertising and synthetic content; operational security governance against foreign interference; and societal-resilience governance through media literacy and strategic communication.

These models are complementary. Effective governance requires coordination between EU institutions, Digital Services Coordinators, national security and communication bodies, independent regulators, fact-checkers, researchers, media organisations, and civil society.

The principal legal constraint is freedom of expression. Disinformation

may be harmful without being illegal. The DSA does not authorise the Commission to invent new prohibited-speech categories (Husovec, 2024). More proportionate tools therefore target systems and conduct: coordinated inauthentic behaviour, non-transparent advertising, undeclared synthetic media, foreign interference, algorithmic amplification, and deficient platform risk management.

National cases show different ways to operationalise this principle. France uses narrow electoral rules and a foreign-interference mandate; Sweden focuses on hostile influence and preparedness; Finland builds citizens' interpretive capacity; Poland and Estonia emphasise monitoring and credible public communication.

Generative AI increases the importance of layered governance because deepfakes, synthetic audio, automated accounts, and mass-generated persuasive text reduce the cost of manipulation. Article 50 of the AI Act responds mainly through transparency and marking, consistent with the wider EU preference for detectability and attribution over general prohibition.

The European Democracy Shield, presented in November 2025, reinforces a whole-of-society approach by linking information-space integrity, election protection, independent media, civil society, and societal resilience (European Commission, 2025b).

The study covers selected Member States and focuses on institutional design rather than quantitative effectiveness. Future research should compare enforcement decisions, platform responses, citizen trust, and measurable exposure to disinformation as the DSA, AI Act, and Democracy Shield mature.

Conclusion. State regulation of disinformation in the EU has evolved toward a multi-layer governance system. EU law does not generally prohibit false information; it regulates platform risks, political-advertising transparency, synthetic-content disclosure, media pluralism, and support for independent verification and research.

Member States complement this framework differently: France combines electoral law with foreign-interference detection; Sweden institutionalises psychological defence; Finland emphasises media literacy; Poland combines communication, reporting, and NASK monitoring; Estonia embeds strategic communication within security and crisis coordination.

Effective governance requires distinguishing false content from coordinated manipulation and systemic amplification. Direct intervention is most defensible where unlawful conduct, electoral manipulation, or foreign interference is clearly defined. For broader lawful but misleading information, transparency, platform accountability, independent fact-checking, media pluralism, and media literacy are more proportionate.

The emerging EU model is therefore resilience-oriented. Its purpose is not to give public authorities a monopoly over truth, but to increase

traceability, reduce opaque manipulation, strengthen institutional and societal capacity, and preserve free and informed democratic debate.

Conflict of interest. The authors declare that the research was conducted in the absence of any commercial, financial, or personal relationships that could be construed as a potential conflict of interest.

Funding. The authors declare that this research was conducted without external funding. The publication costs were covered by the authors themselves.

Ethical aspects. This study was based exclusively on publicly available secondary data, official statistical sources, and published scientific literature. The research did not involve human participants, animal subjects, or the collection of personal data. Therefore, ethical approval was not required. All research procedures were conducted in accordance with generally accepted principles of academic integrity and research ethics.

Generative AI statement. The authors declare that no Generative AI was used in the preparation of this manuscript unless otherwise explicitly stated in the manuscript.

Author contributions. All authors contributed equally to the conceptualisation of the study, research design, data analysis, interpretation of the results, and preparation of the manuscript. All authors reviewed and approved the final version of the manuscript and agreed to be accountable for its content.

Publisher's note. All claims expressed in this article are solely those of the author's and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

Abrusci, E. (2024). The UK Online Safety Act, the EU Digital Services Act and online disinformation: Is the right to political participation adequately protected? Journal of Media Law, 16(2), 440–467. https://doi.org/10.1080/17577632.2024.2425551

Bayer, J. (2024). The EU policy on disinformation: Aims and legal basis. Journal of Media Law, 16(1), 18–27. https://doi.org/10.1080/17577632.2024.2362478

European Commission. (2024). Guidelines for providers of very large online platforms and very large online search engines on the mitigation of systemic risks for electoral processes. https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes

European Commission. (2025a). The Code of Conduct on Disinformation. https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation

European Commission. (2025b). European Democracy Shield and EU Strategy for Civil Society pave the way for stronger and more resilient democracies. https://digital-strategy.ec.europa.eu/en/news/european-democracy-shield-and-eu-strategy-civil-society-pave-way-stronger-and-more-resilient

European Commission. (2026a). Guidelines on transparency obligations for providers and deployers of certain AI systems under Article 50 of the AI Act. https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems

European Commission. (2026b). Code of Practice on Transparency of AI-generated Content. https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content

European Commission. (n.d.). European Digital Media Observatory (EDMO). https://digital-

strategy.ec.europa.eu/en/policies/european-digital-media-observatory
European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union.
European Parliament & Council of the European Union. (2024a). Regulation (EU) 2024/900 on the transparency and targeting of political advertising. Official Journal of the European Union.
European Parliament & Council of the European Union. (2024b). Regulation (EU) 2024/1083 establishing a common framework for media services in the internal market (European Media Freedom Act). Official Journal of the European Union.
European Parliament & Council of the European Union. (2024c). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.
Government of Estonia. (2023). Coalition agreement 2023–2027. https://www.valitsus.ee/en/coalition-agreement-2023-2027
Government Office of Estonia. (2023). Government Office Strategy 2023–2026. https://www.riigikantselei.ee/en/government-office-strategy-2023-2026
Gsenger, R. (2026). Platform governance under the Digital Services Act: A perspective on disinformation. Information, Communication & Society, 29(10), 3037–3055. https://doi.org/10.1080/1369118X.2025.2590561
Husovec, M. (2024). The Digital Services Act's red line: What the Commission can and cannot do about disinformation. Journal of Media Law, 16(1), 47–56. https://doi.org/10.1080/17577632.2024.2362483
Ministry of Digital Affairs of Poland. (2026). Jak walczymy z dezinformacją [How we counter disinformation]. https://www.gov.pl/web/cyfryzacja/jak-walczymy-z-dezinformacja
Nannini, L., Bonel, E., Bassi, D., & Maggini, M. J. (2025). Beyond phase-in: Assessing impacts on disinformation of the EU Digital Services Act. AI and Ethics, 5, 1241–1269. https://doi.org/10.1007/s43681-024-00467-w
National Audiovisual Institute. (2019). Media literacy in Finland: National media education policy. https://kavi.fi/en/publications/
NASK. (2026). Disinformation Analysis Center. https://oad.nask.pl/en
Psychological Defence Agency. (n.d.). Our mission. https://mpf.se/psychological-defence-agency/about-us/our-mission
Republic of France. (2018). Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. Légifrance.
VIGINUM. (2026). Les missions de VIGINUM [The missions of VIGINUM]. Secrétariat général de la défense et de la sécurité nationale. https://www.sgdsn.gouv.fr/viginum/comprendre-viginum/les-missions-de-viginum