



# Media Sovereignty and Information Integrity

## A European Framework for Democratic Information Systems

*Protecting democracy through transparency, pluralism, cognitive resilience and information integrity.*

### Executive Summary

The ability of democratic societies to produce, verify and evaluate trustworthy information has become one of the defining strategic challenges of the twenty-first century. Information is no longer merely a public good or a commercial product. It has become critical strategic infrastructure, alongside energy, finance, technology and defence. Societies that lose the capacity to maintain independent and trustworthy information environments gradually lose the capacity to exercise sovereign democratic judgement.

Europe faces a profound structural transformation of its information ecosystem. Public trust in media and institutions continues to decline, while ownership concentration, commercial incentives, political influence, algorithmic amplification, artificial intelligence and organised influence operations increasingly shape the information environment through which citizens perceive reality. The resulting challenge is not primarily ideological but systemic. It concerns the integrity of the democratic information infrastructure itself.

This paper argues that freedom of expression, although indispensable, is no longer sufficient on its own. Democratic resilience also requires information integrity—a framework of transparency, plurality, accountability and cognitive resilience that enables citizens to evaluate information independently while fully preserving freedom of opinion, open debate and editorial independence.

The paper introduces the concept of **media sovereignty** as Europe's capacity to maintain an independent, pluralistic and trustworthy information ecosystem capable of supporting informed democratic decision-making. Media sovereignty does not imply governmental control over information or protectionism against foreign ideas. It seeks to strengthen the institutional conditions under which democratic freedom can genuinely flourish.

To achieve this objective, the paper proposes a comprehensive **European Information Integrity Framework** based on mutually reinforcing principles and institutions. These include transparency of ownership and funding, public registers of significant influence, an independent Information Integrity Index, voluntary European media certification supported by a European Code of Information Integrity, democratic public oversight, transparency of algorithms and AI-generated content, disclosure of foreign influence, civic participation in media evaluation, education for cognitive resilience, protection against psychological violence and the establishment of an independent European Information Authority responsible for monitoring the structural integrity of Europe's information ecosystem.

The paper further argues that the information ecosystem should be recognised as **critical public infrastructure**. As with energy, finance or digital networks, democratic societies require



resilient information systems capable of providing reliable and transparent information during crises, hybrid attacks, armed conflicts and other emergencies. Protecting information integrity therefore becomes an essential component of democratic resilience.

Psychological aggression—including organised manipulation, cognitive engineering, disinformation campaigns and information warfare—is presented as a strategic challenge to democratic governance. Modern societies require legal, educational and institutional mechanisms capable of protecting not only physical security but also the cognitive conditions necessary for free and informed democratic choice. For this reason, the paper proposes the development of a European Convention on Protection Against Psychological Violence as part of Europe's broader democratic security architecture.

The proposals presented in this document are neither a programme for censorship nor a new system of media regulation. They constitute a strategic framework designed to strengthen transparency, public trust and democratic accountability while fully respecting freedom of expression, political pluralism and editorial independence. The objective is not to regulate opinions, but to protect the integrity of the information environment within which opinions are formed.

Ultimately, the paper argues that democratic sovereignty rests upon a sequential chain of resilience. Media sovereignty strengthens information integrity. Information integrity enables epistemological sovereignty. Epistemological sovereignty supports cognitive sovereignty. Cognitive sovereignty ultimately becomes the foundation of Europe's strategic sovereignty. A society that cannot independently generate, verify and evaluate trustworthy information cannot preserve informed democratic choice, long-term legitimacy or strategic autonomy.

Protecting Europe's information space is therefore not a restriction of democracy. It is one of its essential preconditions.

## **1. Information Has Become Strategic Infrastructure**

For most of modern history, infrastructure was understood primarily in physical terms. Roads, ports, energy networks, financial systems and communication lines formed the foundations upon which economic development, national security and political stability depended. In the twenty-first century, however, information has become an equally critical strategic infrastructure. The ability to generate, process, distribute and evaluate information increasingly determines the capacity of societies to govern themselves, compete economically and defend their sovereignty.

Digital technologies have fundamentally transformed the way citizens perceive reality. Information is no longer transmitted through a limited number of newspapers, broadcasters or public institutions. It flows continuously through digital platforms, search engines, social networks, artificial intelligence systems and algorithmic recommendation mechanisms that influence billions of decisions every day. The infrastructure through which societies understand the world has therefore become as strategically important as the infrastructure through which they transport energy or goods.

Artificial intelligence further accelerates this transformation. Algorithms increasingly determine what individuals read, watch and discuss, while generative AI can produce



persuasive content at unprecedented speed and scale. The distinction between authentic information, synthetic content and coordinated influence operations is becoming progressively more difficult to identify. As a result, the struggle for influence has shifted from controlling territory to shaping perception.

Information has consequently become a strategic resource. States, corporations, political organisations and foreign actors compete not only for markets or military advantage but also for the capacity to influence public opinion, social behaviour and political decision-making. Information operations, psychological influence campaigns, algorithmic amplification and digital manipulation are no longer exceptional activities; they have become permanent features of international competition.

This transformation requires a corresponding evolution in European strategic thinking. Information should no longer be regarded solely as a matter of media policy or freedom of expression. It must also be recognised as a critical component of Europe's strategic infrastructure, deserving the same level of resilience, transparency and protection as energy systems, financial markets, telecommunications or critical digital networks.

The relationship between information and sovereignty has therefore fundamentally changed. Democratic sovereignty depends upon the ability of citizens to make informed decisions. If the information environment is systematically manipulated, democratic procedures may continue formally while becoming progressively less capable of reflecting independent public judgement. Information integrity is thus no longer simply a media issue; it has become a prerequisite for democratic legitimacy.

For this reason, media sovereignty cannot be understood as state control over information or protectionism against foreign ideas. It is the capacity of a democratic society to maintain an information environment in which citizens are able to access diverse sources, evaluate competing interpretations independently and reach political conclusions free from systematic manipulation. Information integrity therefore becomes the operational foundation of cognitive sovereignty, while cognitive sovereignty itself becomes an essential precondition for Europe's strategic sovereignty.

## **Information Ecosystem as Critical Infrastructure**

Like energy grids, transport networks and financial systems, the information ecosystem has become critical public infrastructure. Democratic societies increasingly depend upon reliable information flows for effective governance, economic activity, crisis management and democratic participation.

Protecting information infrastructure therefore extends beyond safeguarding digital networks or communication technologies. It also requires preserving the integrity, resilience and continuity of the information environment itself. During natural disasters, public health emergencies, armed conflicts or hybrid attacks, citizens must retain access to reliable, pluralistic and verifiable information.

Recognising the information ecosystem as strategic public infrastructure does not diminish freedom of expression. On the contrary, it helps preserve the conditions under which free expression, informed democratic participation and independent public debate remain possible.



## 2. The Crisis of the European Information Space

Europe's information environment is experiencing a profound structural transformation. The crisis is not primarily technological, political or ideological. It is systemic. It concerns the architecture through which information is produced, distributed and interpreted, and the growing inability of that architecture to sustain informed democratic decision-making.

Public trust in traditional media has steadily declined across much of Europe. Confidence in political institutions, journalism and expert communities has weakened, while citizens increasingly question the credibility of information itself. At the same time, the volume of available information has expanded exponentially. The challenge is no longer access to information but the capacity to distinguish reliable knowledge from manipulation, propaganda, commercial persuasion and organised psychological influence.

Ownership concentration has further narrowed the diversity of information ecosystems. Although Europe formally enjoys a plurality of media outlets, many depend upon similar news agencies, financial structures, technological platforms or advertising markets. Editorial independence is frequently constrained by commercial pressures, political interests or institutional incentives rather than direct censorship. Public broadcasters often operate under varying degrees of governmental influence, while commercial media increasingly compete for audience attention through emotional engagement rather than analytical depth. Digital platforms, meanwhile, optimise visibility according to algorithmic criteria designed primarily to maximise user engagement rather than public understanding.

These structural incentives encourage sensationalism, emotional polarisation and the simplification of complex issues. Headlines increasingly replace analysis, speed replaces verification, and attention becomes more valuable than accuracy. Serious public debate is displaced by continuous cycles of controversy, outrage and personalised conflict, while long-term strategic questions receive comparatively limited attention. Investigative journalism, traditionally one of the principal safeguards of democratic accountability, faces increasing financial and institutional pressures, reducing its capacity to challenge centres of power independently.

The digital environment amplifies these dynamics. Social media platforms personalise information flows according to behavioural profiles, reinforcing existing preferences and creating fragmented information ecosystems in which different groups are exposed to increasingly different versions of reality. Algorithmic recommendation systems reward emotionally engaging content, irrespective of its contribution to informed democratic deliberation. Artificial intelligence further accelerates both the production and dissemination of persuasive content, making manipulation more sophisticated and increasingly difficult to detect.

These developments have produced an information environment characterised by abundance but declining coherence, unprecedented connectivity but growing fragmentation, and greater access to content accompanied by diminishing confidence in its reliability. The result is not simply misinformation or political polarisation. It is a gradual erosion of the shared informational foundation upon which democratic societies depend.



The European information crisis should therefore not be understood as a conflict between particular political viewpoints or competing ideological positions. It is a structural crisis of the information ecosystem itself. Without restoring transparency, plurality, accountability and public trust, Europe will find it increasingly difficult to sustain informed democratic debate, social cohesion and independent strategic decision-making.

### 3. Media as a Driver of Cognitive Dependence

The principal function of the media in democratic society has traditionally been to inform citizens, facilitate public debate and provide independent scrutiny of political and economic power. In the contemporary information environment, however, the media increasingly perform an additional and far more influential role: they shape the cognitive framework through which societies interpret reality.

This transformation has profound implications for democratic sovereignty. Political decisions are not based solely on objective facts but on how those facts are perceived, interpreted and prioritised. The process through which societies construct these perceptions is therefore no longer merely a matter of journalism or communication; it has become a strategic determinant of political behaviour and democratic legitimacy.

This paper defines **cognitive dependence** as a condition in which individuals or societies progressively lose the capacity to evaluate reality according to their own experience, historical memory, cultural traditions and independent judgement. Instead, perceptions, priorities and political choices become increasingly influenced by externally constructed cognitive frameworks that are accepted without sufficient critical evaluation.

Cognitive dependence rarely develops through direct coercion. It emerges gradually through a process that may be described as **cognitive engineering**: the systematic and often non-transparent shaping of perception, interpretation and decision-making through communication, education, media, digital technologies and institutional influence. Its objective is not necessarily to convince citizens of a specific opinion, but to define the boundaries within which opinions are formed.

Modern information systems possess numerous mechanisms through which cognitive engineering operates. Agenda setting determines which issues receive public attention and which remain largely invisible. Framing influences how those issues are interpreted before citizens begin their own evaluation. Editorial selection decides which facts, experts and perspectives become publicly legitimate, while repetition reinforces particular narratives until familiarity itself becomes a substitute for credibility. Digital algorithms amplify these effects by prioritising content that maximises engagement, emotional response or behavioural prediction rather than informational value.

The cumulative result is the formation of **narratives**—coherent interpretative frameworks through which societies understand complex events. Narratives are not inherently false. They often combine verified facts with selective emphasis, omission and emotional framing, presenting one interpretation as the natural or morally unquestionable understanding of reality. Once widely replicated across media, academic institutions, political communication and digital platforms, narratives increasingly define the limits of acceptable public discourse.



Digital technologies have significantly accelerated this process. Recommendation algorithms personalise information according to behavioural profiles, reinforcing existing preferences while reducing exposure to competing interpretations. The resulting **echo chambers** gradually narrow cognitive diversity and strengthen confirmation bias. Artificial intelligence further increases the scale and sophistication of content generation, allowing persuasive narratives to be produced, adapted and disseminated almost instantaneously across multiple audiences.

These processes are not driven by a single actor or central authority. Governments, international organisations, commercial media, digital platforms, universities, think tanks, non-governmental organisations, corporations and, in some cases, intelligence services all contribute—intentionally or unintentionally—to shaping the contemporary information environment. Their objectives differ, as do their methods and institutional responsibilities. Yet together they form an interconnected ecosystem in which information, influence and legitimacy reinforce one another. Cognitive dependence is therefore an emergent property of the system itself rather than the product of one organisation or ideology.

The consequences extend beyond media consumption. When citizens are continuously exposed to increasingly homogeneous interpretative frameworks, democratic pluralism gradually weakens. Public debate becomes narrower, independent verification declines, and political choices increasingly reflect pre-structured cognitive environments rather than autonomous judgement. Democratic institutions may continue to function procedurally while progressively losing the independent cognitive foundation upon which meaningful democratic choice depends.

This is why the challenge facing Europe cannot be reduced to combating misinformation or protecting freedom of expression alone. The deeper challenge concerns the integrity of the cognitive environment in which democratic decisions are formed. A society that cannot independently generate, verify and critically evaluate knowledge inevitably becomes vulnerable to external influence, psychological manipulation and strategic dependence.

The media no longer simply report reality. They increasingly participate in constructing the reality upon which democratic decisions are based. Protecting Europe's information environment therefore means protecting the cognitive conditions of democratic sovereignty itself.

#### **4. Why Existing Media Models Are No Longer Sufficient**

The contemporary European information environment is shaped primarily by three institutional models: government-funded public media, commercially owned private media and global digital platforms. Each performs an important democratic function, yet each is also subject to structural dependencies that limit its capacity to safeguard information integrity.

Government-funded media were originally established to provide reliable public-interest journalism independent of commercial pressures. In practice, however, their institutional independence often depends upon political appointment procedures, public financing mechanisms and regulatory frameworks determined by governments or parliamentary majorities. Even where editorial autonomy is formally protected, perceptions of political influence can undermine public confidence and contribute to declining institutional trust.



Commercial media operate under a different set of incentives. Their primary dependence is economic rather than political. Competition for advertising revenue, audience attention and digital engagement increasingly favours emotionally compelling content, rapid publication and simplified narratives. Investigative journalism, long-form analysis and complex policy reporting often struggle to compete with commercially optimised information formats. As advertising markets become increasingly concentrated within global technology platforms, commercial media face additional pressures that further influence editorial priorities.

Digital platforms represent a third and fundamentally different model. Unlike traditional media organisations, platforms generally do not produce most of the content they distribute. Instead, they determine its visibility through proprietary recommendation algorithms designed to maximise engagement, user retention and commercial value. These algorithms have become powerful gatekeepers of public attention despite operating according to criteria that remain largely opaque to citizens, researchers and democratic institutions. Their influence extends beyond distribution; they increasingly shape public agendas, social interactions and the overall architecture of democratic discourse.

Each of these models contributes valuable functions to democratic society, yet none is institutionally neutral. Government media are vulnerable to political dependence. Commercial media are vulnerable to commercial dependence. Digital platforms are vulnerable to algorithmic dependence. These dependencies do not necessarily imply intentional manipulation or institutional failure. Rather, they represent structural characteristics that influence how information is selected, prioritised and presented.

The challenge is therefore not to replace one model with another. No single ownership structure or institutional arrangement can guarantee objective information. Democratic resilience requires a pluralistic ecosystem in which different models coexist within a framework of transparency, accountability and public oversight.

Europe's objective should not be greater control over information but greater integrity of the information environment. Freedom of expression remains indispensable, yet freedom alone cannot ensure that citizens possess the conditions necessary for informed democratic judgement. A resilient democracy requires not only free media but also transparent institutions, accountable information systems and citizens capable of evaluating competing sources independently.

**All three existing models generate structural conflicts of interest. None, by themselves, provide sufficient protection for democratic information integrity. The challenge for Europe is therefore not to choose between them, but to establish a common framework that strengthens transparency, pluralism and public trust across them all.**

## **5. Principles of European Information Integrity**

Europe requires a new information doctrine capable of protecting democratic freedom without undermining it. The objective is not to regulate opinions or determine political truth, but to preserve the conditions under which free citizens can independently evaluate information, participate in public debate and make sovereign democratic decisions. Information integrity therefore complements, rather than limits, freedom of expression.



The first principle is **freedom of expression**. Open debate remains the cornerstone of every democratic society. Citizens must remain free to express opinions, challenge institutions and present competing interpretations of reality. The protection of democracy can never be achieved by suppressing legitimate disagreement.

Freedom alone, however, is insufficient. It must be accompanied by **plurality**. Democratic societies require genuine diversity of viewpoints, methodologies and information sources. Pluralism is not measured by the number of media outlets but by the diversity of independent perspectives available to citizens. An information ecosystem dominated by identical narratives, even when produced by multiple organisations, cannot fulfil this democratic function.

Plurality depends upon **transparency**. Citizens have the right to know who owns media organisations, who finances think tanks and civil society organisations, how digital platforms prioritise information and what interests stand behind influential public campaigns. Transparency does not determine credibility; it enables citizens to assess credibility independently.

Transparency must be supported by **accountability**. Media organisations, digital platforms and institutions that shape public opinion should be accountable for their professional standards, correction procedures and disclosure of conflicts of interest. Accountability does not imply political supervision but public responsibility proportional to their influence upon democratic decision-making.

The principle of **subsidiarity** should also guide information governance. Decisions concerning media regulation should be taken at the lowest effective democratic level, while strategic challenges such as cross-border disinformation, foreign influence operations and algorithmic transparency require coordinated European action. National diversity and European cooperation should reinforce rather than undermine one another.

Information integrity further depends upon **source verification**. Democratic debate requires that information be traceable, evidence-based and open to independent verification wherever possible. Citizens should be encouraged to compare multiple sources, distinguish facts from interpretation and understand the difference between reporting, commentary and opinion.

Closely related is **editorial independence**. Journalism fulfils its democratic role only when editorial decisions are protected from political, commercial and ideological interference. Genuine independence requires not merely legal guarantees but institutional arrangements capable of safeguarding professional judgement from external pressure.

The same applies to **ownership transparency**. Concentrated ownership, hidden financial interests or opaque funding structures reduce public confidence regardless of editorial quality. Citizens should always know who ultimately controls significant information channels and whose interests may be represented.

In the digital age, transparency must extend beyond ownership to include **algorithmic transparency**. Recommendation systems increasingly determine which information becomes visible and which remains marginal. While proprietary technologies deserve protection, the principles governing content prioritisation, political advertising, artificial intelligence and automated amplification should remain open to independent democratic scrutiny.



Ultimately, the resilience of democratic societies depends upon their citizens. **Cognitive resilience**—the ability to evaluate information critically, recognise manipulation and resist psychological pressure—has become a strategic civic competence. Education should therefore cultivate critical thinking, media literacy, digital literacy and an understanding of artificial intelligence alongside traditional democratic education.

Finally, information integrity cannot exist without **protection against psychological violence**. Systematic manipulation, organised intimidation, coercive information campaigns and cognitive engineering directly undermine individual autonomy and democratic decision-making. Just as democratic societies protect citizens from physical violence, they must also develop legal, institutional and educational mechanisms capable of protecting the cognitive conditions upon which democratic freedom depends.

Together, these principles constitute the foundation of a European Information Integrity Framework. They neither replace media freedom nor weaken democratic pluralism. Rather, they create the conditions under which freedom, plurality and democratic sovereignty can continue to exist in an increasingly complex information environment.

## **Freedom and Information Integrity**

Information integrity should never be interpreted as determining what citizens should think or believe. Its purpose is to protect the conditions under which individuals remain free to form independent opinions through access to transparent, pluralistic and verifiable information.

Freedom of expression and information integrity are therefore complementary rather than competing principles. One protects the freedom to communicate; the other protects the integrity of the information environment within which democratic deliberation takes place.

## **6. Protection Against Psychological Violence**

Modern democracies have developed comprehensive legal frameworks to protect individuals against physical violence, recognising that human dignity cannot exist where bodily integrity is systematically threatened. Yet the twenty-first century has demonstrated that violence no longer targets only the body. Psychological aggression has become an increasingly sophisticated instrument capable of influencing individuals, destabilising societies and weakening democratic institutions without the use of physical force.

Psychological violence should therefore be understood as the systematic use of manipulation, intimidation, deception or coercive influence intended to undermine individual autonomy, distort informed decision-making or erode democratic trust. It extends beyond interpersonal abuse to include organised campaigns of disinformation, cognitive engineering, algorithmic manipulation, coordinated intimidation, information warfare and other forms of psychological aggression directed against individuals, communities or entire societies.

At the **personal level**, the objective is protection and resilience. Citizens should possess the same right to protection against severe psychological aggression as they already enjoy against physical violence. Legal systems should recognise psychological harm where systematic manipulation, intimidation or coercion demonstrably threatens human dignity or personal autonomy. At the same time, education must equip citizens with the intellectual tools necessary



to resist manipulation through critical thinking, media literacy, digital self-defence and the development of psychological resilience. The strongest protection remains an individual capable of recognising attempts to manipulate perception before they influence behaviour.

At the **societal level**, democratic institutions must protect the integrity of the public sphere itself. Information systems that systematically reward manipulation, organised deception or coordinated psychological influence gradually weaken social trust and democratic legitimacy. Independent oversight mechanisms should therefore monitor information integrity, encourage transparency and identify organised psychological aggression without becoming instruments of political censorship. Particular attention should be given to algorithmic amplification, covert influence operations, hidden financial interests and non-transparent networks capable of shaping public perception without democratic accountability. The objective is not to regulate opinions but to preserve the conditions for genuinely free public debate.

At the **European level**, psychological aggression has become a strategic security issue. Modern information warfare increasingly seeks to influence elections, polarise societies, undermine confidence in democratic institutions and weaken Europe's capacity for independent decision-making. Such operations may originate from state actors, non-state organisations, commercial interests or transnational influence networks. Europe therefore requires a coordinated legal and institutional response that recognises psychological aggression as an integral dimension of democratic security.

This paper proposes the development of a **European Convention on Protection Against Psychological Violence**, complementing existing human rights instruments by establishing common legal definitions, minimum standards of protection and mechanisms for international cooperation. The Convention should distinguish clearly between legitimate democratic persuasion and organised psychological aggression while preserving freedom of expression and political pluralism. Its purpose is not to regulate political opinion but to protect the cognitive conditions necessary for democratic choice.

Protection against psychological violence should ultimately become a recognised component of European strategic policy alongside defence, cybersecurity, energy security and economic resilience. Military aggression seeks to control territory; psychological aggression seeks to control perception. Both threaten sovereignty, although by different means.

Europe's strategic autonomy will therefore depend not only upon military capability, technological innovation or economic competitiveness, but also upon its ability to preserve the mental independence of its citizens and the integrity of its democratic information environment. A society capable of recognising and resisting systematic psychological manipulation protects far more than individual well-being—it protects the foundations of democracy itself.

The protection of Europe begins not only at its physical borders but also within its cognitive space. Safeguarding citizens against psychological violence is therefore not merely a social responsibility; it is an essential condition of European democratic resilience and strategic sovereignty.

7.2 Information Integrity Index Independent European methodology. Evaluation based upon: • transparency • ownership • corrections • sources • editorial independence • plurality • algorithm transparency



7.3 European Media Certification Voluntary certification. Professional standards. Independent auditing. Recognition rather than licensing.

7.4 Democratic Public Oversight Independent Information Integrity Councils. Representatives from: journalism academia law technology citizens civil society No governmental control.

7.5 Transparency of Algorithms Independent audits. Disclosure obligations. Political advertising. AI systems. Recommendation principles.

## **7. A European Information Integrity Framework**

The challenges described in the previous chapters cannot be addressed through isolated regulatory measures or national initiatives alone. Europe's information environment has become transnational, technologically integrated and strategically significant. Protecting democratic decision-making therefore requires a coherent institutional framework capable of strengthening transparency, accountability and public trust while fully respecting freedom of expression and editorial independence.

The objective of a European Information Integrity Framework is neither to regulate opinions nor to determine political truth. Democratic societies remain founded upon open debate and intellectual diversity. The purpose is instead to create institutional conditions under which citizens can evaluate information independently, understand who influences public discourse and distinguish transparent communication from organised manipulation.

The framework proposed in this paper is therefore based on transparency rather than censorship, accountability rather than political control, and democratic resilience rather than information restriction.

### **7.1 Transparency of Ownership and Funding**

The credibility of democratic information depends not only upon what is communicated but also upon who communicates it and whose interests are represented. Citizens cannot evaluate information independently if the structures of ownership and influence remain opaque.

All significant actors participating in the European information environment should therefore operate under comprehensive transparency obligations. These should apply not only to media organisations but also to digital platforms, think tanks, policy institutes, major advocacy organisations and non-governmental organisations actively engaged in shaping public policy.

Disclosure should include ownership structures, beneficial ownership, principal funding sources, significant foreign financing, institutional partnerships and political affiliations where relevant. Commercial sponsorship, lobbying activities and strategic communication contracts should likewise be publicly identifiable.

Transparency does not imply suspicion. International cooperation, philanthropy and foreign partnerships remain legitimate features of democratic society. The objective is simply to ensure that citizens possess sufficient information to evaluate potential conflicts of interest independently and to understand the institutional context in which public narratives are formed.



## **European Register of Significant Influence**

Transparency should extend beyond media ownership alone. A publicly accessible European register should disclose significant ownership structures, principal funding sources and relevant institutional affiliations of organisations exercising substantial influence on public opinion or public policy.

The register could include major media organisations, digital platforms, think tanks, research institutes, large advocacy organisations and other entities whose activities significantly shape public debate. Its objective would not be to restrict participation in democratic life but to strengthen transparency, accountability and informed public trust.

## **7.2 European Information Integrity Index**

Democratic societies regularly evaluate the quality of education, healthcare, financial stability and environmental performance. The integrity of the information environment deserves similar objective assessment.

A European Information Integrity Index should therefore be developed using transparent, publicly available methodology and independent scientific oversight. Its purpose would not be to evaluate political opinions or ideological positions, but to measure institutional characteristics that contribute to trustworthy public communication.

Indicators could include transparency of ownership and funding, disclosure of conflicts of interest, editorial independence, correction procedures, diversity of sources, methodological transparency, separation between reporting and opinion, algorithmic accountability and professional journalistic standards.

The Index would function as a public information instrument rather than a regulatory mechanism. It would provide citizens, researchers and policymakers with objective indicators regarding institutional transparency and information integrity while encouraging continuous professional improvement throughout the European information ecosystem.

## **7.3 European Media Certification**

Professional credibility increasingly requires standards that extend beyond legal compliance. Europe should therefore establish a voluntary system of European Media Certification recognising organisations that demonstrate exceptional commitment to transparency, editorial independence and professional integrity.

Certification should remain entirely voluntary and should never become a prerequisite for publication or participation in public debate. Its purpose is recognition rather than licensing. Media organisations choosing to participate would undergo periodic independent evaluation according to publicly available professional criteria.

Assessment would consider editorial governance, transparency of financing, correction policies, source verification procedures, protection of editorial independence, algorithmic disclosure where applicable and adherence to recognised ethical standards.



Such certification would not determine which media citizens should trust. Rather, it would provide an additional signal of institutional commitment to professional responsibility, allowing audiences to make more informed choices while encouraging higher standards throughout the sector.

## European Code of Information Integrity

Voluntary certification should be supported by a European Code of Information Integrity establishing common professional standards for organisations wishing to demonstrate their commitment to trustworthy information practices.

The Code could include commitments to:

- transparency of ownership and funding;
- clear separation of reporting, analysis and opinion;
- prompt correction of factual errors;
- transparency regarding significant use of artificial intelligence in editorial processes;
- editorial independence from political and commercial influence.

Participation would remain entirely voluntary. Compliance would strengthen public confidence while preserving editorial freedom and institutional independence.

## 7.4 Democratic Public Oversight

Democratic oversight of the information environment should never become governmental control over journalism. Equally, however, an information ecosystem exercising significant influence over democratic life cannot remain entirely without independent public accountability.

For this reason, the European Information Integrity Framework proposes the establishment of independent **Information Integrity Councils** operating at both European and national levels. Their composition should reflect the diversity of democratic society, bringing together representatives from journalism, academia, law, technology, civil society and citizens through transparent appointment procedures designed to minimise political influence.

The Councils would possess neither censorship powers nor editorial authority. Their responsibilities would instead include monitoring structural developments within the information environment, publishing annual assessments, overseeing methodological standards for the Information Integrity Index, supervising voluntary certification processes and issuing public recommendations concerning transparency, algorithmic accountability and emerging risks to democratic information integrity.

Their legitimacy would derive from independence, methodological transparency and public confidence rather than political authority.



## 7.5 Transparency of Algorithms

Algorithms have become among the most influential editors in modern democratic society. They increasingly determine which information citizens encounter, which topics dominate public debate and which perspectives remain largely invisible.

Despite this influence, algorithmic decision-making often remains inaccessible to democratic scrutiny. The principles governing recommendation systems, content prioritisation, political advertising, automated moderation and artificial intelligence are frequently protected as proprietary commercial information, leaving citizens unable to understand how their information environment is shaped.

The European Information Integrity Framework therefore proposes proportionate transparency obligations for major digital platforms. These should include disclosure of the general principles governing recommendation systems, political advertising, automated content amplification, artificial intelligence applications and moderation policies, while fully respecting legitimate commercial confidentiality and intellectual property rights.

Independent European audits should verify compliance with these transparency obligations without requiring disclosure of proprietary source code. Their objective would not be to interfere with technological innovation but to ensure that algorithmic systems exercising significant democratic influence remain compatible with principles of transparency, accountability and public trust.

Algorithmic transparency is ultimately not a technological issue but a democratic one. In societies where algorithms increasingly shape public perception, understanding the principles through which they influence information becomes an essential condition for informed democratic citizenship.

## Transparency of AI-Generated Content

As artificial intelligence becomes increasingly integrated into journalism, public communication and digital platforms, citizens should be able to distinguish between human-created and AI-generated content whenever technically feasible.

Transparent identification of AI-assisted content strengthens public trust without restricting innovation. The objective is not to regulate ideas or opinions, but to provide citizens with sufficient contextual information to evaluate the origin and reliability of digital information.

## 7.6 Foreign Influence Transparency

International cooperation is an essential characteristic of open democratic societies. European institutions, universities, foundations, media organisations and civil society benefit from cooperation with partners around the world. Openness, however, cannot justify opacity. Democratic legitimacy requires that citizens understand who finances, organises and influences public debate.

The European Information Integrity Framework therefore proposes comprehensive transparency requirements for foreign influence activities affecting the European public sphere.



These should apply equally to foreign state actors, publicly funded institutions, strategic communication organisations, foundations, lobbying organisations, policy institutes, non-governmental organisations and other entities that actively seek to influence public policy or public opinion within the European Union.

Disclosure should include sources of funding, institutional affiliations, strategic partnerships, contractual relationships and the objectives of organised influence campaigns. Such transparency should apply irrespective of the country of origin or political orientation of the organisation concerned. Democratic legitimacy requires equal standards for all actors.

The objective is not to restrict international cooperation or civil society activity. On the contrary, transparent cooperation strengthens public confidence. Citizens should be able to distinguish between independent civic initiatives and organised influence operations designed to advance external political, ideological or commercial interests.

Transparency therefore becomes an instrument of democratic resilience rather than political control.

## **7.7 European Public Media Reform**

The concept of public media requires fundamental reconsideration. In many European countries, public broadcasters have gradually become identified either with governments or with political majorities, while commercial media increasingly depend upon advertising markets and audience metrics. Neither model fully satisfies the democratic function originally assigned to public service journalism.

Europe should therefore redefine public media as independent public service institutions whose primary responsibility is to serve citizens rather than governments, political parties or commercial interests.

Their constitutional mandate should include editorial independence, balanced reporting, methodological transparency, diversity of viewpoints, long-term investigative journalism and protection from both political and commercial interference. Governance structures should minimise political appointments through independent and transparent selection procedures, while financing mechanisms should guarantee long-term editorial autonomy.

The purpose of public media is not to compete for audience attention through sensationalism or ideological positioning. Their primary role is to strengthen the quality of democratic debate by providing reliable information, contextual analysis and genuine pluralism. Public trust can only be restored when public media are perceived as institutions serving society rather than the interests of governments or political coalitions.

## **7.8 Civic Evaluation**

Democratic information systems should not be evaluated exclusively by governments, regulators or media professionals. Citizens themselves constitute the primary stakeholders of the information environment and should therefore participate in assessing its quality and credibility.



For this purpose, the paper proposes the establishment of a **European Civic Media Observatory**, enabling citizens to contribute structured evaluations of media performance through transparent and scientifically validated methodologies.

Citizen assessments should focus on institutional characteristics rather than political agreement, including perceived transparency, factual reliability, diversity of viewpoints, editorial accountability, correction practices and public trust. These evaluations would complement, rather than replace, professional assessment mechanisms and academic research.

The Observatory would generate public indicators of confidence in European information systems, allowing long-term monitoring of trust, credibility and institutional performance. Such democratic feedback would strengthen accountability while encouraging continuous improvement across the European media landscape.

## 7.9 Education for Cognitive Resilience

No regulatory framework can replace an informed and intellectually resilient citizenry. The most effective protection against manipulation remains the individual's capacity to recognise it.

Education should therefore become the first line of defence against cognitive dependence. Alongside traditional civic education, European educational systems should systematically develop critical thinking, media literacy, digital literacy, artificial intelligence literacy, source verification skills and psychological resilience.

Citizens should learn how narratives are constructed, how algorithms influence information exposure, how confirmation bias operates and how organised influence campaigns exploit cognitive vulnerabilities. Understanding these mechanisms strengthens democratic participation without prescribing political conclusions.

Cognitive resilience is not scepticism towards all information. It is the disciplined ability to evaluate competing claims independently through evidence, logic and multiple sources. A society possessing this competence becomes substantially more resistant to disinformation, psychological manipulation and information warfare while remaining fully committed to democratic openness.

## 7.10 European Convention on Protection Against Psychological Violence

The growing strategic significance of psychological aggression requires an international legal response comparable to existing conventions protecting individuals against physical violence and safeguarding fundamental human rights.

This paper therefore proposes a **European Convention on Protection Against Psychological Violence**, establishing common legal definitions, minimum standards of protection and coordinated mechanisms for prevention, investigation and international cooperation.

The Convention should distinguish clearly between legitimate democratic persuasion, freedom of expression and organised psychological aggression intended to manipulate, intimidate or systematically undermine democratic decision-making. It should provide legal protection for



individuals while also recognising that coordinated psychological influence may threaten democratic institutions and national sovereignty.

The Convention would further strengthen European resilience against information warfare, foreign influence operations, coercive strategic communication and emerging forms of cognitive manipulation enabled by artificial intelligence and digital technologies.

By recognising psychological violence as a legitimate subject of European and international law, Europe would acknowledge that the protection of democratic societies extends beyond physical security to include the cognitive conditions upon which democratic freedom depends.

## 7.11 European Information Authority

To ensure coherence across the proposed framework, Europe should establish an independent **European Information Authority (EIA)** as a specialised institution responsible for safeguarding the integrity of the European information environment.

The Authority should possess a status comparable to other independent European agencies such as the **European Central Bank**, the **European Medicines Agency** and the **European Environment Agency**. Its independence from governments, political parties, commercial interests and media organisations would constitute its principal source of legitimacy.

The European Information Authority would not regulate journalistic content, approve political opinions or determine what citizens are permitted to read or publish. It would exercise no censorship powers and would not function as a ministry of information.

Its responsibilities would instead focus on monitoring the structural integrity of Europe's information ecosystem. These responsibilities would include developing and maintaining the European Information Integrity Index, administering voluntary media certification, monitoring structural developments within the information environment, publishing annual European Information Integrity Reports, conducting strategic risk assessments, monitoring the impact of artificial intelligence on democratic communication, coordinating independent algorithm audits, monitoring foreign influence operations, developing common methodological standards, supporting scientific research and issuing recommendations to European institutions and Member States.

Beyond its analytical responsibilities, the Authority should contribute to strengthening Europe's resilience during major crises, including natural disasters, pandemics, cyber incidents, hybrid attacks and armed conflicts. Its role would not be to direct public communication, but to facilitate cooperation, transparency and the timely exchange of verified information between European and national institutions.

The Authority would also serve as a European centre of expertise on cognitive resilience, information integrity and democratic information systems, facilitating cooperation among researchers, regulators, civil society, technology experts and media professionals.

Its mission would be straightforward: **to protect the democratic information infrastructure upon which European freedom depends.**



The European Information Authority would therefore represent not a new instrument of state control, but a new institution of democratic protection—strengthening transparency, accountability and public trust while fully respecting freedom of expression, editorial independence and political pluralism.

## 8. Information Integrity as the Foundation of Cognitive Sovereignty

The proposals presented in this paper are not intended merely to improve the quality of journalism or strengthen media regulation. They address a much broader strategic objective: restoring Europe's capacity for independent democratic judgement.

The twenty-first century has fundamentally altered the relationship between information and sovereignty. Political communities no longer lose autonomy only through military defeat or economic dependence. They may also lose it gradually by becoming cognitively dependent upon information environments whose priorities, narratives and standards of legitimacy are increasingly shaped beyond their own democratic control.

For this reason, media sovereignty should not be understood simply as protecting national media industries or promoting European digital platforms. Its true purpose is to safeguard the integrity of the information environment within which democratic societies form opinions, evaluate evidence and make political decisions.

Information integrity represents the first institutional layer of this process. Without transparency, plurality, editorial independence, methodological accountability and public trust, democratic debate becomes progressively more vulnerable to manipulation. Information integrity therefore provides the conditions necessary for genuine knowledge production.

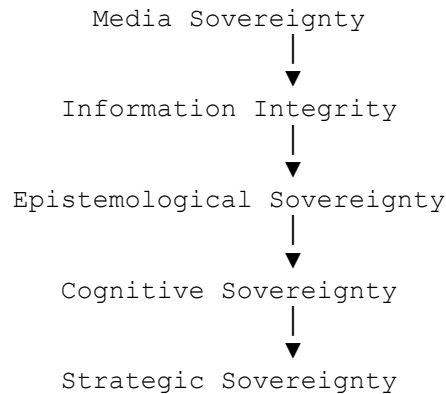
From this foundation emerges **epistemological sovereignty**—the capacity of a society to produce, verify and develop knowledge according to rigorous scientific standards and its own intellectual traditions. Universities, research institutions, independent journalism and scientific communities all contribute to this capacity. A civilisation that no longer generates its own knowledge gradually becomes dependent upon intellectual frameworks developed elsewhere.

Epistemological sovereignty enables **cognitive sovereignty**. Citizens who can access trustworthy information, critically evaluate competing interpretations and understand the mechanisms of manipulation retain the ability to form independent judgements. Democratic choice becomes meaningful because it is based upon autonomous reasoning rather than externally structured perception.

Only societies possessing cognitive sovereignty can achieve **strategic sovereignty**. Independent foreign policy, technological competitiveness, defence capabilities and economic resilience ultimately depend upon independent political judgement. Strategic autonomy begins long before governments formulate policy—it begins in the information environment through which societies understand reality itself.



These relationships form a coherent chain of democratic resilience:



Each level depends upon the integrity of the preceding one. A society that cannot independently produce, verify and evaluate information cannot make sovereign democratic decisions. Likewise, a political union that remains cognitively dependent cannot become strategically sovereign regardless of its economic resources or military capabilities.

Europe's strategic renewal therefore begins not only with institutional reform, technological innovation or defence policy, but with restoring the cognitive conditions necessary for democratic self-government.

## 9. Implementation Roadmap

Transforming Europe's information environment requires gradual institutional evolution rather than abrupt regulatory intervention. The proposed European Information Integrity Framework should therefore be implemented progressively, allowing democratic adaptation, institutional learning and continuous evaluation.

### Phase One – Transparency and Democratic Accountability

The first phase should establish the legal foundations of information integrity through comprehensive transparency legislation. Priority should be given to ownership disclosure, beneficial ownership registers, transparency of funding, disclosure of foreign influence activities and algorithmic transparency for major digital platforms.

This phase does not regulate content. It strengthens the democratic principle that citizens have the right to understand who influences the information environment within which they form political judgements.

### Phase Two – Institutional Capacity

Once transparency mechanisms are established, Europe should create the institutional infrastructure necessary to support long-term information integrity.

This phase includes the establishment of the European Information Authority, development of the European Information Integrity Index, implementation of voluntary European Media Certification, creation of Information Integrity Councils and systematic education for cognitive resilience throughout European educational systems.



The objective is to strengthen democratic capacity rather than administrative control.

### **Phase Three – European and International Cooperation**

The final phase extends information integrity beyond the European Union itself.

Europe should initiate a European Convention on Protection Against Psychological Violence while promoting international cooperation against information warfare, organised psychological aggression and emerging forms of artificial intelligence-enabled manipulation.

Common European standards should gradually become reference standards for democratic information governance internationally, strengthening both European sovereignty and global democratic resilience.

The implementation process should remain transparent, evidence-based and subject to continuous democratic review. The objective is not institutional expansion for its own sake but the gradual construction of a resilient European information environment capable of supporting democratic legitimacy for future generations.

## **10. Conclusion**

### **Information Integrity Is the Foundation of Democratic Legitimacy**

Europe's democratic future depends not only upon free elections, constitutional institutions or economic prosperity. It depends equally upon the quality of the information environment through which citizens understand reality, evaluate competing ideas and make political decisions.

The digital transformation of the twenty-first century has fundamentally altered this environment. Information has become strategic infrastructure, algorithms have become influential editors, artificial intelligence increasingly shapes public communication and organised cognitive influence has become a permanent feature of geopolitical competition. Democracies must therefore evolve accordingly.

The purpose of this paper has not been to advocate greater control over information. On the contrary, democratic freedom can only flourish where information remains pluralistic, transparent and intellectually trustworthy. Freedom of expression remains inviolable. Yet freedom alone cannot protect democracy if citizens are deprived of the conditions necessary to exercise independent judgement.

The proposed European Information Integrity Framework seeks to strengthen those conditions. Through transparency, accountability, pluralism, cognitive resilience and protection against psychological violence, Europe can preserve an information environment capable of supporting informed democratic choice while remaining fully committed to openness and political diversity.

The challenge is ultimately civilisational rather than technological. A society that loses confidence in its capacity to distinguish knowledge from manipulation gradually loses confidence in democracy itself. Restoring trust therefore requires more than combating



disinformation. It requires rebuilding the institutional foundations of Europe's cognitive independence.

Without trustworthy information there can be no informed citizens.

Without informed citizens there can be no meaningful democratic choice.

Without meaningful democratic choice there can be no cognitive sovereignty.

Without cognitive sovereignty there can be no strategic sovereignty.

Europe cannot remain politically sovereign while remaining cognitively dependent upon external information systems.

**The protection of Europe's information space is therefore not a restriction of democracy. It is one of the essential preconditions for its survival.**

## Appendix A

### Timeline of Information Operations (1948–Present)

#### *The evolution from strategic propaganda to cognitive engineering*

The history of modern information operations demonstrates a gradual but profound transformation in the methods through which states, institutions, corporations and technological platforms influence public perception. What began as centrally organised propaganda has evolved into complex, decentralised systems of strategic communication, algorithmic amplification and artificial intelligence-assisted cognitive influence.

This timeline does not imply that every operation was coordinated or pursued identical objectives. Rather, it illustrates how information has progressively become a strategic domain comparable to diplomacy, economics and military power. The cumulative effect of these developments has been the emergence of information as critical strategic infrastructure and cognitive influence as an increasingly important instrument of statecraft.

| Year        | Event / Operation                      | Strategic Objective                        | Principal Actors                                           | Long-term Significance                                                        |
|-------------|----------------------------------------|--------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------|
| 1948        | Operation Mockingbird                  | Strategic influence through media networks | CIA, U.S. media                                            | Demonstrated the strategic importance of media influence during the Cold War. |
| 1950s–1960s | Influence operations in Western Europe | Counter Soviet political influence         | United States, European governments, intelligence services | Information campaigns become an integral part of geopolitical competition.    |



| Year      | Event / Operation                        | Strategic Objective                                    | Principal Actors                                       | Long-term Significance                                                                             |
|-----------|------------------------------------------|--------------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| 1971      | Nixon Shock                              | Preservation of monetary dominance                     | United States                                          | Demonstrated the close relationship between economic power, communication and strategic influence. |
| 1980s     | Expansion of global satellite television | Global information distribution                        | International broadcasters                             | Beginning of transnational real-time information ecosystems.                                       |
| 1989–1991 | Collapse of the Soviet bloc              | Democratic transition and institutional transformation | Western governments, international organisations, NGOs | Information and institutional influence become key instruments of political transformation.        |
| 1990s     | Internet commercialisation               | Global digital communication                           | Technology companies                                   | Information begins shifting from traditional media to digital networks.                            |
| 1990s     | Expansion of international NGO networks  | Democratic assistance and governance programmes        | International foundations, NGOs                        | Civil society becomes an increasingly important actor within information ecosystems.               |
| 2001      | September 11 and the Patriot Act         | Counter-terrorism and expanded surveillance            | United States                                          | Security, intelligence and digital communications become increasingly interconnected.              |
| 2003      | Iraq War                                 | Strategic communication during military intervention   | Coalition governments, international media             | Raised global debate concerning media independence and information verification.                   |
| 2004–2008 | Rise of social media platforms           | Global digital communication                           | Google, Meta, YouTube                                  | Platform algorithms begin replacing editorial gatekeepers.                                         |
| 2013      | Snowden disclosures                      | Public awareness of digital surveillance               | NSA, Edward Snowden                                    | Growing concerns regarding digital sovereignty and privacy.                                        |
| 2016      | Cambridge Analytica                      | Behavioural targeting in political campaigns           | Cambridge Analytica, Facebook                          | Public recognition of large-scale data-driven political influence.                                 |
| 2020      | COVID-19 pandemic                        | Crisis communication and public health governance      | WHO, governments, media, platforms                     | Demonstrated the strategic importance of information governance                                    |



| Year         | Event / Operation                  | Strategic Objective                             | Principal Actors                                     | Long-term Significance                                                                                             |
|--------------|------------------------------------|-------------------------------------------------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
|              |                                    |                                                 |                                                      | during global emergencies.                                                                                         |
| 2022         | War in Ukraine                     | Information warfare and strategic communication | Russia, Ukraine, NATO, EU institutions, global media | Cognitive influence becomes recognised as an integral dimension of modern conflict.                                |
| 2023–Present | Generative Artificial Intelligence | Automated knowledge production and influence    | OpenAI, Google, Anthropic, Microsoft and others      | AI fundamentally transforms the scale, speed and sophistication of information production and cognitive influence. |

## Historical Evolution of Information Operations

The timeline illustrates five distinct phases in the evolution of information influence:

### Phase I (1948–1989): Strategic Propaganda

Information operations were primarily state-centred, relying on traditional media, broadcasting and intelligence-supported communication.

### Phase II (1990–2003): Global Information Networks

Globalisation, democratisation and the expansion of international media created interconnected information systems operating across national borders.

### Phase III (2004–2015): Platform Dominance

Digital platforms gradually replaced traditional media as the principal distributors of information. Algorithms became increasingly influential in determining public visibility.

### Phase IV (2016–2022): Behavioural Influence

Large-scale data analytics, algorithmic recommendation systems and coordinated digital communication transformed information into a strategic instrument capable of influencing political behaviour at unprecedented scale.

### Phase V (2023–Present): Cognitive Engineering

Artificial intelligence, generative content and autonomous recommendation systems increasingly influence not only what societies know, but how they construct reality itself. Information operations are evolving from communication strategies into comprehensive systems of cognitive engineering.



## Strategic Observation

The evolution presented in this appendix demonstrates that information has progressively moved from being a supporting element of political communication to becoming an independent strategic domain.

The defining trend is not the emergence of misinformation or propaganda—both have existed throughout history—but the increasing capacity to shape perception through technologically integrated ecosystems that combine media, digital platforms, artificial intelligence, behavioural analytics, strategic communication and institutional influence.

This historical evolution provides the context for the concept of **cognitive dependence** developed in this paper. As the means of shaping perception become more sophisticated, protecting democratic societies requires moving beyond the traditional concept of media freedom toward a broader framework of **information integrity, cognitive resilience and cognitive sovereignty**.

## Appendix B

### Case Study: COVID-19 and Information Governance

#### *Lessons for democratic resilience in the digital age*

The COVID-19 pandemic represented the largest global information challenge since the emergence of the internet. Alongside the public health emergency developed an unprecedented information crisis involving governments, international organisations, scientific institutions, traditional media, digital platforms and technology companies. Never before had so many institutions attempted simultaneously to inform, persuade and regulate public behaviour on such a global scale.

The pandemic demonstrated both the necessity of coordinated communication and the vulnerabilities of contemporary democratic information systems. It showed how rapidly scientific uncertainty can become politicised, how digital platforms can shape public discourse through algorithmic moderation, and how declining public trust may undermine even well-intentioned public policies.

This case study does not evaluate medical decisions or public health policies. Rather, it examines how information was produced, communicated and governed during a period of exceptional uncertainty, and what lessons can be drawn for future democratic resilience.

### Scientific Uncertainty and Public Communication

Scientific knowledge developed rapidly throughout the pandemic. Recommendations concerning face masks, transmission pathways, school closures, natural immunity, vaccine effectiveness and booster programmes evolved as new evidence became available.

Such adaptation represents a normal characteristic of scientific inquiry. However, scientific uncertainty was frequently communicated through simplified political narratives that often presented evolving recommendations as settled scientific consensus. When official guidance



later changed, many citizens interpreted these revisions not as normal scientific progress but as institutional inconsistency, contributing to declining public confidence.

The experience demonstrated that democratic communication should distinguish more clearly between established scientific evidence, expert consensus and areas of legitimate uncertainty.

## **Platform Governance and Content Moderation**

Digital platforms became central actors in pandemic communication. Companies such as Google, Meta, YouTube and X (formerly Twitter) introduced extensive moderation policies intended to limit the spread of health misinformation and promote information from recognised public authorities.

While these measures sought to protect public health, they also generated significant debate regarding freedom of expression, scientific pluralism and the appropriate relationship between governments, digital platforms and private content moderation.

Several scientists and medical professionals whose views diverged from prevailing public recommendations experienced content restrictions, account suspensions or reduced algorithmic visibility. Regardless of the scientific merits of individual cases, these developments highlighted the growing influence of private technology companies over democratic information flows.

The pandemic therefore illustrated the need for greater transparency regarding platform governance rather than relying exclusively on discretionary moderation practices.

## **Institutional Coordination**

The pandemic also revealed unprecedented coordination between governments, international organisations, public health agencies, traditional media and digital platforms.

Institutions such as the **World Health Organization (WHO)**, the **European Medicines Agency (EMA)**, national public health authorities and governmental crisis headquarters became primary reference points for public communication. Mainstream media largely relied upon these institutions as principal sources, while digital platforms promoted official guidance through dedicated information panels and algorithmic prioritisation.

Such coordination may be necessary during major emergencies. Nevertheless, the experience demonstrated the importance of preserving independent scientific debate and transparent evaluation even under exceptional circumstances. Democratic resilience depends upon maintaining public confidence not only through coordinated communication but also through openness to evidence, methodological transparency and the possibility of legitimate professional disagreement.

## **Public Trust**

Perhaps the most significant long-term consequence of the pandemic concerned public trust.



In many countries, confidence in governments, media organisations, scientific institutions and digital platforms declined during and after the pandemic. Public opinion became increasingly polarised, with disagreement extending beyond public health policy into broader questions of institutional credibility, democratic legitimacy and freedom of expression.

The pandemic demonstrated that trust cannot be sustained solely through institutional authority. It depends equally upon transparency, accountability, consistency and the willingness of institutions to communicate uncertainty openly.

## **Lessons for Information Integrity**

Several lessons emerge from the COVID-19 experience.

First, crisis communication should distinguish clearly between scientific evidence, expert judgement and political decision-making.

Second, digital platform governance requires greater transparency regarding moderation policies, algorithmic prioritisation and cooperation with public authorities.

Third, democratic societies should preserve conditions for responsible scientific debate even during emergencies.

Fourth, information resilience depends upon citizens capable of critically evaluating multiple sources rather than relying exclusively upon any single authority.

Finally, the pandemic demonstrated that information governance has become a strategic component of democratic resilience. Future crises—whether involving public health, security, artificial intelligence or climate change—will require institutions capable of balancing coordinated public communication with transparency, pluralism and intellectual openness.

## **Strategic Observation**

The COVID-19 pandemic illustrated that modern crises are simultaneously biological, technological, political and informational.

It demonstrated that information governance has become a strategic capability comparable to public health preparedness or civil protection. Democracies require not only effective emergency communication but also institutional mechanisms capable of preserving transparency, public trust and cognitive resilience under conditions of uncertainty.

The principal lesson is therefore not about the pandemic itself, but about the future.

Europe's resilience will increasingly depend upon its ability to manage crises without compromising the transparency, pluralism and information integrity upon which democratic legitimacy ultimately rests.



## Selected Public Assessments

The COVID-19 pandemic generated one of the most extensive public debates in recent history concerning scientific transparency, institutional accountability, information governance and the relationship between governments, technology platforms and public communication. While many questions remain contested, several official institutions, independent commissions and prominent public figures have highlighted issues directly relevant to information integrity and democratic resilience.

### Official Assessments

Several official investigations and institutional reviews have reached conclusions that underline the importance of transparency and independent scrutiny.

- The **U.S. Intelligence Community** concluded in 2021 that the available evidence was insufficient to determine the origin of SARS-CoV-2 with confidence, with agencies reaching different assessments.
- In January 2025, the **CIA** revised its public assessment, stating that a research-related (laboratory) origin appeared more likely than natural spillover, while explicitly assigning **low confidence** to this judgement and maintaining that both scenarios remained plausible pending further evidence.
- Congressional investigations in the United States examined government decision-making, the origins of the pandemic, cooperation between public authorities and digital platforms, and the transparency of public health communication. These investigations contributed to broader debates regarding democratic oversight and institutional accountability.

These assessments demonstrate that uncertainty itself became an important feature of the information environment and that transparent communication regarding uncertainty is essential for maintaining public trust.

### Academic Perspectives

A number of internationally recognised scholars argued that the pandemic revealed structural weaknesses in the relationship between science, public policy and information governance.

Jeffrey Sachs, Chair of the *Lancet COVID-19 Commission*, repeatedly argued that the origins of SARS-CoV-2 required a fully independent international investigation and that scientific transparency was indispensable for maintaining public confidence. The Commission ultimately concluded that both natural spillover and a research-related incident remained plausible hypotheses requiring further investigation.

John Ioannidis emphasised the importance of evidence-based policymaking, proportionality of public health measures and openness to scientific debate throughout the pandemic.

Jay Bhattacharya argued that democratic societies should preserve scientific pluralism during public emergencies and warned that suppressing legitimate scientific disagreement could undermine long-term public trust.



Although these scholars often disagreed on specific policy questions, they shared a common concern regarding transparency, open scientific debate and the preservation of independent inquiry.

## **Public Policy Perspectives**

Several political leaders and senior public officials subsequently argued that the pandemic exposed broader governance problems extending beyond public health.

Tulsi Gabbard has argued that greater transparency is required regarding intelligence assessments, public decision-making and interactions between government institutions and digital platforms during the pandemic. She has also supported further disclosure of information relating to the origins of COVID-19 and the handling of intelligence assessments.

Other policymakers in Europe and North America have similarly called for stronger parliamentary oversight, clearer separation between scientific advice and political decision-making, and greater transparency concerning cooperation between governments, technology companies and public health authorities.

## **Lessons for Democratic Information Governance**

The significance of these assessments does not lie primarily in resolving every scientific or political controversy surrounding the pandemic. Rather, they illustrate a broader lesson for democratic governance.

Major crises inevitably generate uncertainty, evolving evidence and difficult policy choices. Under such conditions, democratic resilience depends less on unanimous agreement than on transparent institutions, open scientific inquiry, independent oversight and public confidence that competing hypotheses can be examined without political or institutional pressure.

The COVID-19 experience therefore reinforces one of the central arguments of this paper: **information integrity requires transparency, methodological openness and the protection of independent scientific and public debate.** Without these conditions, public trust erodes, cognitive dependence increases and democratic legitimacy is weakened.

## **Appendix C**

### **Case Study: The Information Environment of the War in Ukraine**

#### ***Information warfare as a strategic dimension of modern conflict***

The war in Ukraine represents the most significant information conflict in Europe since the end of the Cold War. Military operations have been accompanied by an unprecedented struggle to influence public perception, political decision-making and international legitimacy. Information has become an operational domain alongside diplomacy, economics, cyber operations and conventional military power.



This case study does not seek to determine political responsibility for the conflict, nor does it assess military operations. Its purpose is to examine how modern information ecosystems function during international crises and what lessons can be drawn for democratic information integrity.

## Competing Strategic Narratives

From the outset, the conflict was accompanied by competing strategic narratives.

The dominant Western narrative emphasised:

- Russian military aggression.
- Ukraine's right to self-defence.
- Protection of the international rules-based order.
- European solidarity.
- Sanctions and military assistance.

The Russian official narrative emphasised:

- NATO enlargement.
- Security guarantees requested by Russia before 2022.
- Protection of Russian-speaking populations.
- The implementation failure of the Minsk Agreements.
- The conflict as part of a broader geopolitical confrontation.

Neither narrative fully explains the complexity of the conflict. Each highlights certain facts while assigning less attention to others. This illustrates one of the central characteristics of modern information environments: narratives are constructed through selection, emphasis and interpretation rather than through fabrication alone.

## Information Governance During the Conflict

The conflict also produced unprecedented measures affecting the European information environment.

Among the most significant developments were:

- the suspension of Russian state broadcasters within the European Union;
- restrictions on RT and Sputnik distribution;
- extensive platform moderation policies;
- prioritisation of official governmental communication;
- coordinated strategic communication by NATO and EU institutions;
- increased use of open-source intelligence (OSINT);
- extensive use of social media by governments, military institutions and individual actors.

These developments demonstrated that information itself became an operational component of the conflict.



## **The Role of Digital Platforms**

Unlike previous wars, the conflict unfolded largely in real time through digital platforms.

Algorithms determined which videos, images and interpretations achieved global visibility.

Artificial intelligence increasingly assisted:

- translation;
- content production;
- information verification;
- image analysis;
- disinformation detection;
- propaganda production.

Digital platforms therefore became strategic actors despite remaining private commercial companies.

## **Strategic Communication**

Governments, international organisations, armed forces, NGOs, think tanks and media organisations all invested heavily in strategic communication.

Information campaigns sought to:

- maintain domestic public support;
- influence international opinion;
- justify political decisions;
- strengthen alliances;
- weaken adversary legitimacy;
- mobilise economic and military assistance.

Strategic communication therefore became an integral component of national security.

## **Lessons for Democratic Information Integrity**

The conflict demonstrates several broader lessons.

First, modern conflicts are simultaneously military and cognitive.

Second, democratic societies require greater transparency concerning information sources, strategic communication and organised influence activities.

Third, citizens increasingly depend upon digital platforms whose algorithms remain largely outside democratic oversight.

Fourth, independent source verification becomes more important than ever during periods of war, when emotional mobilisation naturally increases.



Finally, protecting democratic debate requires distinguishing between legitimate strategic communication, journalism, public diplomacy and organised psychological influence.

## **Documented Historical Context**

Several documented developments continue to influence interpretations of the conflict and remain relevant for understanding the contemporary information environment.

These include:

- the commitments discussed during German reunification concerning NATO enlargement;
- the NATO Bucharest Summit (2008);
- the political changes in Ukraine in 2014;
- the Minsk I and Minsk II Agreements;
- public statements by former German Chancellor Angela Merkel and former French President François Hollande regarding the implementation of the Minsk process;
- the negotiations held in Istanbul in March–April 2022;
- subsequent decisions regarding continued military support and sanctions.

These events are documented through official agreements, public statements and diplomatic records. Their interpretation remains contested, illustrating precisely why pluralism of sources and independent historical analysis remain essential components of democratic information integrity.

## **Strategic Observation**

The war in Ukraine demonstrates that information has become a strategic theatre of modern conflict.

Military operations seek control over territory.

Information operations seek control over perception.

Strategic communication seeks control over legitimacy.

Artificial intelligence increasingly accelerates all three.

For democratic societies, the principal lesson is not which narrative ultimately prevails, but whether citizens retain the capacity to evaluate competing claims independently through transparent evidence, multiple sources and open public debate.

Without that capacity, democratic decision-making becomes progressively vulnerable to cognitive dependence regardless of the military outcome of the conflict.



## Appendix D

### Mechanisms of Narrative Formation

#### *How modern information ecosystems shape public perception*

Modern democratic societies are influenced not only by facts but by the interpretative frameworks through which those facts are understood. These frameworks—commonly referred to as narratives—provide meaning, establish priorities and define what is considered legitimate knowledge within public discourse.

Narratives are not necessarily false. Most are built upon factual information. Their influence derives not from fabrication but from the selective organisation, interpretation and repetition of facts within coherent explanatory frameworks. As a result, citizens often disagree not because they possess different facts but because they interpret the same facts through different narratives.

Narrative formation has therefore become one of the principal mechanisms through which contemporary information environments shape democratic decision-making. Understanding this process is essential for preserving cognitive sovereignty.

#### The Narrative Formation Process

Modern narratives emerge through a multi-layered process involving numerous independent actors rather than a single coordinating authority. Political institutions, scientific organisations, think tanks, media organisations, universities, civil society organisations, technology companies and digital platforms each contribute to the construction and dissemination of public meaning.

The process typically follows several interconnected stages.

##### 1. Event or Issue

Every narrative begins with an event requiring interpretation.

Examples include:

- military conflicts;
- pandemics;
- migration crises;
- elections;
- economic shocks;
- technological breakthroughs.

Facts alone do not determine public understanding.

Interpretation begins immediately.



## 2. Agenda Setting

Only a limited number of issues receive sustained public attention.

Governments, international organisations, media organisations, think tanks and digital platforms all influence which subjects dominate public discussion and which receive comparatively little attention.

Agenda setting therefore determines **what society discusses**.

## 3. Framing

Once an issue enters public debate, it must be interpreted.

Framing provides the cognitive structure through which citizens understand events.

Typical frames include:

- democracy versus authoritarianism;
- security versus freedom;
- science versus misinformation;
- solidarity versus nationalism;
- crisis versus opportunity.

Framing influences **how society understands the issue**.

## 4. Source Selection

Information is then supported through selected authorities.

These may include:

- governments;
- international organisations;
- universities;
- scientific experts;
- NGOs;
- think tanks;
- intelligence assessments;
- recognised journalists.

Source selection strongly influences credibility because institutional authority often substitutes for independent verification.

## 5. Narrative Amplification

Once established, narratives are amplified across multiple information channels.

These include:



- news agencies;
- television;
- newspapers;
- digital media;
- social networks;
- search engines;
- podcasts;
- influencers;
- educational institutions.

Repetition gradually transforms interpretation into perceived consensus.

## **6. Algorithmic Reinforcement**

Digital platforms personalise information through recommendation algorithms.

Rather than exposing citizens to competing viewpoints, algorithms frequently reinforce previous interests and behavioural preferences.

This creates:

- confirmation bias;
- echo chambers;
- emotional amplification;
- behavioural prediction;
- selective visibility.

Algorithms increasingly influence not only information distribution but public attention itself.

## **7. Social Internalisation**

Repeated exposure normalises particular interpretations.

Citizens begin to reproduce narratives voluntarily through:

- interpersonal discussion;
- workplaces;
- schools;
- universities;
- professional organisations;
- political parties;
- civil society.

At this stage narratives become embedded within social identity rather than remaining external communication.

## **8. Political Decision-Making**

Ultimately, narratives influence democratic outcomes.

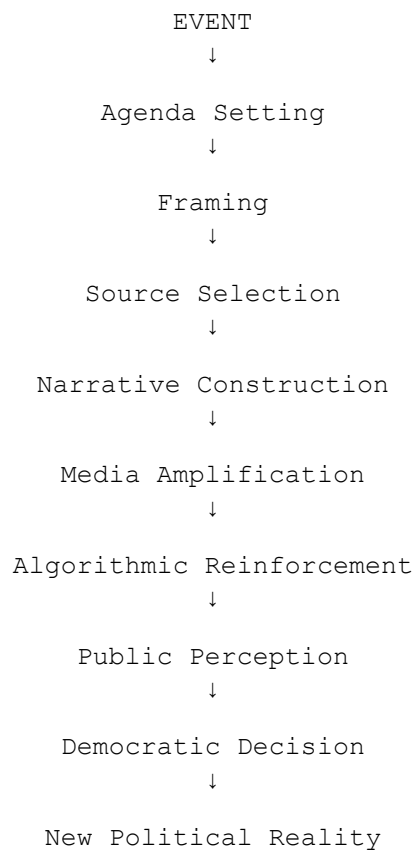


They shape:

- electoral preferences;
- legislative priorities;
- foreign policy;
- public spending;
- institutional legitimacy;
- social cohesion.

Political decisions therefore emerge from cognitive environments constructed long before citizens enter the voting booth.

## Narrative Formation Cycle



### Narrative Formation and Cognitive Engineering

Narrative formation is a normal feature of every democratic society.

Cognitive engineering begins when narrative construction becomes systematic, non-transparent and strategically designed to influence perception without the informed awareness of citizens.

Unlike traditional propaganda, cognitive engineering rarely relies upon direct censorship.



Instead it operates through:

- selective visibility;
- prioritisation;
- repetition;
- emotional framing;
- algorithmic amplification;
- institutional authority;
- behavioural targeting;
- social conformity.

Its objective is not simply to persuade citizens.

Its objective is to shape the cognitive environment within which persuasion becomes possible.

## **Strategic Observation**

Narratives are indispensable for democratic life because societies require shared frameworks through which complex realities become understandable.

The democratic challenge therefore does not lie in eliminating narratives but in ensuring that they emerge within transparent, pluralistic and intellectually open information environments.

Where multiple independent narratives can compete freely, citizens retain the capacity for autonomous judgement.

Where narrative formation becomes concentrated, opaque or systematically manipulated, cognitive dependence gradually replaces cognitive sovereignty.

Protecting democratic societies therefore requires safeguarding not only freedom of expression, but also the integrity of the processes through which narratives are formed, challenged and continuously re-evaluated.

## **Appendix E**

### **European Information Integrity Indicators**

#### ***Proposed indicators for evaluating democratic information systems***

A resilient democratic information environment cannot be assessed solely through media freedom rankings or freedom of expression indicators. Modern information systems are shaped by a much broader set of institutional, technological and societal factors that together determine the quality, transparency and trustworthiness of public information.

The European Information Integrity Framework therefore proposes a comprehensive set of **Information Integrity Indicators** designed to evaluate the structural characteristics of national and European information ecosystems.



The indicators do **not** assess political opinions, editorial positions or ideological orientation. Instead, they measure the institutional conditions that enable citizens to receive, verify and evaluate information independently.

Together, these indicators provide the foundation for the proposed **European Information Integrity Index**.

## Indicator Framework

| No. | Indicator                             | Description                                                                                                                 |
|-----|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 1   | <b>Freedom of Expression</b>          | Protection of free speech, editorial freedom and absence of political censorship.                                           |
| 2   | <b>Media Pluralism</b>                | Diversity of independent media ownership, viewpoints and information sources.                                               |
| 3   | <b>Ownership Transparency</b>         | Public disclosure of beneficial ownership and control of media organisations.                                               |
| 4   | <b>Funding Transparency</b>           | Disclosure of public funding, advertising, sponsorship, lobbying and foreign financial support.                             |
| 5   | <b>Editorial Independence</b>         | Institutional safeguards protecting editorial decisions from political or commercial interference.                          |
| 6   | <b>Source Verification</b>            | Professional standards for verification, attribution, corrections and evidence-based reporting.                             |
| 7   | <b>Correction Accountability</b>      | Transparent correction policies and public handling of factual errors.                                                      |
| 8   | <b>Algorithm Transparency</b>         | Disclosure of recommendation principles, political advertising and AI-assisted content distribution.                        |
| 9   | <b>Foreign Influence Transparency</b> | Public reporting of foreign state funding, strategic partnerships and organised influence activities.                       |
| 10  | <b>AI Governance</b>                  | Transparency regarding the use of artificial intelligence in content production, moderation and recommendation systems.     |
| 11  | <b>Psychological Safety</b>           | Institutional capacity to identify and address organised psychological manipulation while protecting freedom of expression. |
| 12  | <b>Public Trust</b>                   | Measured citizen confidence in media institutions and the information environment.                                          |
| 13  | <b>Media Literacy</b>                 | National capacity for media literacy, critical thinking and information verification.                                       |
| 14  | <b>Digital Literacy</b>               | Citizens' ability to understand digital platforms, algorithms and AI systems.                                               |
| 15  | <b>Cognitive Resilience</b>           | Society's capacity to recognise manipulation, evaluate competing narratives and maintain informed democratic judgement.     |



# Indicator Categories

To facilitate analysis, the indicators are organised into five strategic dimensions.

## A. Democratic Foundations

- Freedom of Expression
- Editorial Independence
- Media Pluralism

These indicators assess whether democratic debate can develop freely.

## B. Transparency

- Ownership Transparency
- Funding Transparency
- Foreign Influence Transparency

These indicators evaluate whether citizens understand who shapes the information environment.

## C. Information Quality

- Source Verification
- Correction Accountability
- AI Governance

These indicators measure the professional integrity of information production.

## D. Digital Information Environment

- Algorithm Transparency
- Platform Accountability
- Digital Literacy

These indicators examine the influence of digital technologies on democratic communication.

## E. Democratic Resilience

- Public Trust
- Media Literacy
- Cognitive Resilience
- Protection Against Psychological Violence

These indicators assess society's long-term capacity to preserve democratic decision-making.

## Illustrative Evaluation Scale



| Score    | Interpretation                    |
|----------|-----------------------------------|
| 90–100   | Very High Information Integrity   |
| 75–89    | High Information Integrity        |
| 60–74    | Moderate Information Integrity    |
| 45–59    | Structural Vulnerabilities        |
| Below 45 | High Risk of Cognitive Dependence |

## Guiding Principles

The proposed indicators are founded upon several methodological principles:

- **Political neutrality** – evaluation focuses on institutional characteristics rather than political viewpoints.
- **Transparency** – methodologies, criteria and data sources must be publicly available.
- **Comparability** – results should enable comparison across Member States and over time.
- **Scientific validity** – indicators should be developed in cooperation with academic institutions and independent experts.
- **Periodic review** – methodologies should be updated regularly to reflect technological and societal developments.

## Strategic Purpose

The purpose of these indicators is not to rank political systems according to ideological preferences, but to strengthen Europe's democratic resilience by providing objective measures of the quality and integrity of its information environment.

Used together, they would allow policymakers, researchers, media organisations and citizens to identify structural weaknesses, monitor long-term trends and support evidence-based reforms.

Ultimately, information integrity should become a measurable component of democratic governance, just as fiscal stability, environmental sustainability and the rule of law are already assessed through internationally recognised indicators.

A democracy cannot protect what it cannot measure. Measuring information integrity is therefore the first step toward strengthening cognitive sovereignty and safeguarding Europe's democratic future.



## Appendix F

### European Information Integrity Index (EI<sup>3</sup>)

#### *Proposed Methodology*

##### **Purpose**

The European Information Integrity Index (EI<sup>3</sup>) is proposed as a comprehensive analytical framework for evaluating the structural integrity of democratic information systems across the European Union.

Its objective is **not** to assess political opinions, editorial positions or ideological orientation. Rather, the Index measures the institutional, technological and societal conditions that enable citizens to access, verify and evaluate information independently.

The Index is designed to complement—not replace—existing international indicators such as media freedom rankings, rule of law indices and corruption perception indices by introducing a dedicated framework for measuring **information integrity** as a strategic component of democratic resilience.

##### **Methodological Principles**

The methodology is based upon six fundamental principles.

##### **Independence**

The Index must be developed and administered by an independent European institution protected from governmental, political, commercial and media influence.

##### **Transparency**

All indicators, methodologies, weighting criteria, data sources and calculations must be publicly available and independently verifiable.

##### **Political Neutrality**

The Index evaluates institutional characteristics rather than political opinions or editorial positions.

It does not distinguish between political ideologies.

It evaluates transparency, accountability and democratic resilience.

##### **Scientific Validity**

Indicators should be developed in cooperation with universities, research institutes, journalists, statisticians, information scientists, AI experts and legal scholars.



## Comparability

Results should be comparable

- between Member States,
- over time,
- between sectors,
- and across different information ecosystems.

## Periodic Review

The methodology should be reviewed every five years to reflect technological developments, artificial intelligence and changing information environments.

## Structure of the Index

The proposed methodology consists of **five dimensions** comprising **fifteen core indicators**.

| Dimension                       | Weight |
|---------------------------------|--------|
| Democratic Foundations          | 25%    |
| Transparency                    | 20%    |
| Information Quality             | 20%    |
| Digital Information Environment | 20%    |
| Democratic Resilience           | 15%    |

### Dimension I — Democratic Foundations (25%)

Measures whether democratic information can develop freely.

Indicators:

- Freedom of expression
- Editorial independence
- Media pluralism
- Protection of investigative journalism

### Dimension II — Transparency (20%)

Measures institutional openness.

Indicators:

- Ownership transparency
- Funding transparency
- Foreign influence disclosure
- Lobbying transparency



### **Dimension III — Information Quality (20%)**

Measures professional standards.

Indicators:

- Source verification
- Correction mechanisms
- Editorial accountability
- Professional ethics

### **Dimension IV — Digital Information Environment (20%)**

Measures technological governance.

Indicators:

- Algorithm transparency
- AI governance
- Political advertising transparency
- Platform accountability

### **Dimension V — Democratic Resilience (15%)**

Measures society's capacity to resist manipulation.

Indicators:

- Public trust
- Media literacy
- Digital literacy
- Cognitive resilience
- Protection against psychological violence

### **Scoring Methodology**

Each indicator is scored on a scale from **0 to 100**.

Scores are calculated using a combination of:

- quantitative statistics,
- legal analysis,
- expert assessment,
- institutional reporting,
- public transparency data,
- citizen surveys.

The weighted average produces a national Information Integrity Score.



# Interpretation

| Score    | Classification                         |
|----------|----------------------------------------|
| 90–100   | Excellent Information Integrity        |
| 75–89    | High Information Integrity             |
| 60–74    | Moderate Information Integrity         |
| 45–59    | Significant Structural Vulnerabilities |
| Below 45 | High Risk of Cognitive Dependence      |

The Index should identify structural strengths and weaknesses rather than assign political judgments.

## Sources of Evidence

The methodology should combine multiple independent sources, including:

- official national statistics;
- European Union institutions;
- academic research;
- independent media studies;
- transparency registers;
- media ownership databases;
- digital platform transparency reports;
- public opinion surveys;
- civil society assessments;
- international organisations.

Reliance on multiple sources reduces methodological bias and improves robustness.

## Publication Process

The European Information Integrity Index should be published annually.

Each report should include:

- overall national score;
- scores by dimension;
- trend analysis;
- comparison with previous years;
- European averages;
- identification of structural risks;
- examples of good practice;
- policy recommendations.

The complete methodology and underlying data should be publicly available.



## Governance

The Index should be developed under the supervision of the proposed **European Information Authority** in cooperation with an independent Scientific Advisory Board composed of experts in journalism, law, political science, communication, artificial intelligence, cybersecurity, sociology and statistics.

Independent peer review should accompany every methodological revision.

## Strategic Function

The European Information Integrity Index is not intended to regulate media content or evaluate political viewpoints.

Its purpose is to provide policymakers, researchers, media organisations and citizens with a reliable instrument for monitoring the health of Europe's democratic information environment.

Like the Rule of Law Index, the Corruption Perceptions Index or environmental performance indicators, it offers evidence-based measurement rather than political judgement.

By identifying structural vulnerabilities early, the Index supports preventive action before declining transparency, concentration of influence or cognitive dependence begin to undermine democratic legitimacy.

Ultimately, the Index provides Europe with a common language for discussing information integrity, democratic resilience and cognitive sovereignty. It transforms these concepts from abstract principles into measurable public policy objectives, enabling evidence-based reform while fully respecting freedom of expression, political pluralism and democratic accountability.

## Figure 1. Declining Trust in News in Europe

**Source:** Reuters Institute, Digital News Report 2024

### Year Trust in News (%)

|      |    |
|------|----|
| 2016 | 50 |
| 2017 | 47 |
| 2018 | 44 |
| 2019 | 42 |
| 2020 | 40 |
| 2021 | 38 |
| 2022 | 36 |
| 2023 | 34 |
| 2024 | 32 |

**Graph:** line chart

**Message**



Public trust in news continues to decline despite unprecedented information availability.

**Figure 2. Europe's Dependence on Non-European Cloud Infrastructure**

**Source:** Synergy Research Group, Cloud Market Share Q4 2023

| Provider                                                             | Headquarters   | Market Share (%) |
|----------------------------------------------------------------------|----------------|------------------|
| Amazon AWS                                                           | United States  | 31               |
| Microsoft Azure                                                      | United States  | 25               |
| Google Cloud                                                         | United States  | 11               |
| Alibaba Cloud                                                        | China          | 4                |
| Other (mostly non-EU)                                                | Various        | 27               |
| Major EU providers (OVHcloud, SAP, Deutsche Telekom T-Systems, etc.) | European Union | ~2               |

**Graph:** bar chart

Europe's digital infrastructure remains overwhelmingly dependent on non-European providers.

**Figure 3. Ownership of Europe's Major Information Platforms**

| Platform      | Owner                | Country       |
|---------------|----------------------|---------------|
| Google Search | Alphabet             | United States |
| YouTube       | Alphabet             | United States |
| Facebook      | Meta                 | United States |
| Instagram     | Meta                 | United States |
| WhatsApp      | Meta                 | United States |
| X             | X Corp.              | United States |
| LinkedIn      | Microsoft            | United States |
| TikTok        | ByteDance            | China         |
| Reddit        | Reddit Inc.          | United States |
| Wikipedia     | Wikimedia Foundation | United States |

**Source**

Company annual reports.

**Graph**

Horizontal bar (countries).

Possible summary:



United States = 8

China = 1

European Union = 0

#### Figure 4. Europe's Information Infrastructure

| Sector                   | Main European Position     |
|--------------------------|----------------------------|
| Search engines           | Predominantly non-European |
| Social media             | Predominantly non-European |
| Video platforms          | Predominantly non-European |
| Cloud infrastructure     | Predominantly non-European |
| AI foundation models     | Predominantly non-European |
| Mobile operating systems | Predominantly non-European |
| Browsers                 | Predominantly non-European |
| Online advertising       | Predominantly non-European |

#### Sources

European Commission

OECD

Synergy Research

StatCounter

Statista

#### Figure 5. Information Ecosystem

| Component            | Dominant Actor                       |
|----------------------|--------------------------------------|
| Search               | Google                               |
| Social Networks      | Meta                                 |
| Video                | YouTube                              |
| Professional Network | LinkedIn                             |
| Messaging            | WhatsApp                             |
| Cloud                | AWS / Azure                          |
| AI                   | OpenAI, Google, Anthropic, Microsoft |
| Mobile OS            | Apple / Google                       |

The majority of Europe's digital information ecosystem is controlled outside the European Union.



## Figure 6. Public Trust Compared

Eurobarometer / OECD

| Institution          | Trust (%) |
|----------------------|-----------|
| Scientists           | ~73       |
| Police               | ~69       |
| Courts               | ~57       |
| EU institutions      | ~49       |
| National governments | ~43       |
| Media                | ~32       |

(Exact dataset to verify before publication.)

## Figure 7. Ownership Concentration (Media)

| Ownership Characteristic         | EU Trend   |
|----------------------------------|------------|
| Cross-media ownership            | Increasing |
| National ownership concentration | High       |
| Dependence on advertising        | High       |
| Dependence on global platforms   | Very high  |
| Local investigative journalism   | Declining  |

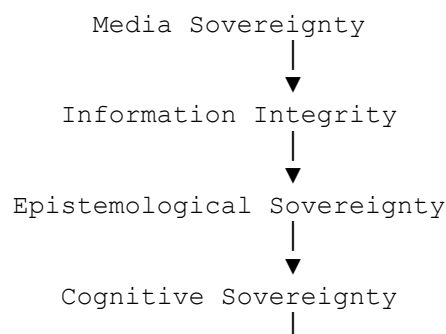
Source:

Media Pluralism Monitor

European Media Freedom Act reports

Centre for Media Pluralism

## Figure 8. Information Integrity Chain





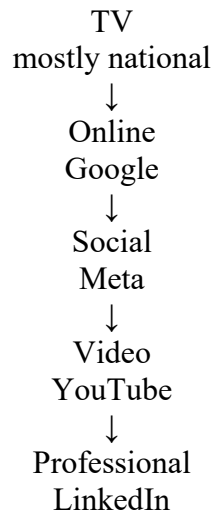
Strategic Sovereignty

## Where Europeans Get Their News

Reuters 2024

| Source               | Share (%) |
|----------------------|-----------|
| Television           | 48        |
| Online news websites | 26        |
| Social media         | 18        |
| Newspapers           | 5         |
| Radio                | 3         |

## Who Controls These Channels



## Figure 9. Ownership of Major Scientific Publishers

| Publisher                  | Headquarters     | Country                      |
|----------------------------|------------------|------------------------------|
| Elsevier                   | Amsterdam (RELX) | Netherlands / United Kingdom |
| Springer Nature            | Berlin / London  | Germany / United Kingdom     |
| Wiley                      | Hoboken          | United States                |
| Taylor & Francis (Informa) | London           | United Kingdom               |
| SAGE Publications          | California       | United States                |
| IEEE                       | New Jersey       | United States                |
| American Chemical Society  | Washington DC    | United States                |
| Oxford University Press    | Oxford           | United Kingdom               |
| Cambridge University Press | Cambridge        | United Kingdom               |
| MDPI                       | Basel            | Switzerland                  |



## Observation

The overwhelming majority of high-impact scientific publishing is controlled by a small number of large publishers headquartered primarily in the United States and the United Kingdom, with limited European Union ownership.

## Sources

- Scopus
- Clarivate
- Company Annual Reports

**Figure 10. Secondary Information Sources Used by European Media**

| Agency                        | Headquarters | Country        |
|-------------------------------|--------------|----------------|
| Reuters                       | London       | United Kingdom |
| Associated Press (AP)         | New York     | United States  |
| Agence France-Presse (AFP)    | Paris        | France         |
| Bloomberg                     | New York     | United States  |
| Deutsche Presse-Agentur (dpa) | Hamburg      | Germany        |
| ANSA                          | Rome         | Italy          |
| EFE                           | Madrid       | Spain          |

## Observation

Most European news organisations rely on a relatively small number of international news agencies as primary secondary information sources.

This creates efficiency but also increases narrative convergence.

**Figure 11. Global Opinion and Financial Publications**

| Publication         | Owner                        | Country        |
|---------------------|------------------------------|----------------|
| The Economist       | The Economist Group          | United Kingdom |
| Financial Times     | Nikkei Inc.                  | Japan          |
| Wall Street Journal | News Corp                    | United States  |
| Washington Post     | Nash Holdings (Jeff Bezos)   | United States  |
| New York Times      | The New York Times Company   | United States  |
| Bloomberg           | Bloomberg LP                 | United States  |
| Foreign Affairs     | Council on Foreign Relations | United States  |
| Foreign Policy      | Graham Holdings              | United States  |



**Figure 12. Knowledge Production Ecosystem**

| Layer                | Dominant Institutions                |
|----------------------|--------------------------------------|
| Scientific journals  | Elsevier, Springer Nature, Wiley     |
| Citation databases   | Scopus, Web of Science               |
| News agencies        | Reuters, AP, AFP                     |
| International media  | Economist, FT, NYT, WSJ              |
| Digital distribution | Google, Meta, X, YouTube             |
| AI systems           | OpenAI, Google, Anthropic, Microsoft |