



LEGAL REGULATION OF PSYCHOLOGICAL VIOLENCE

Comparative Analysis and Future Directions for the Protection of Cognitive Integrity, Cognitive Autonomy and Cognitive Sovereignty

EXECUTIVE SUMMARY

European legal systems increasingly recognize psychological violence as a legitimate subject of legal protection.

This recognition has evolved through multiple legal and regulatory domains, including domestic violence, workplace harassment, anti-discrimination law, consumer protection, data protection, digital platform regulation and artificial intelligence governance.

Despite these developments, regulation remains fragmented. Existing legal frameworks address specific manifestations of psychological violence but lack a coherent framework capable of addressing psychological violence across interpersonal, organizational, political, commercial and digital domains – whether originating from domestic, foreign or transnational actors.

This paper argues that European law is gradually moving toward the protection of a broader legal interest: **cognitive integrity**, understood as the individual's capacity for free, informed and autonomous judgment.

The next stage of legal development may involve the progressive recognition of cognitive autonomy as a protected societal value and the establishment of legal safeguards against forms of psychological violence that systematically undermine independent judgment, democratic resilience and state sovereignty.

The paper does not propose restrictions on freedom of expression or legitimate democratic debate. Rather, it explores whether contemporary legal developments indicate an emerging need to protect the conditions necessary for autonomous thought and decision-making in increasingly complex environments of influence – regardless of whether those influences originate from commercial platforms, domestic institutions, or foreign actors.

1. INTRODUCTION

Modern democratic societies have developed extensive legal protections against physical violence, economic exploitation, discrimination and violations of privacy.

Historically, legal systems focused primarily on protecting life, bodily integrity and property. Constitutional democracies subsequently expanded legal protection to include human dignity, equality, privacy and fundamental rights.



However, contemporary societies face a rapidly evolving challenge.

Advances in mass communication, digital platforms, behavioural technologies, artificial intelligence, algorithmic recommendation systems and large-scale information environments have dramatically increased the capacity of various actors to influence human perception, beliefs, preferences and behaviour. These actors include commercial entities, domestic institutions, foreign state actors, non-state groups, and transnational networks.

Psychological influence itself is neither new nor inherently problematic. Influence is an unavoidable component of social life, democratic politics, education, journalism, culture and commerce.

The challenge emerges when influence becomes systematic, opaque, asymmetrical and capable of significantly impairing autonomous judgment.

Increasingly, forms of psychological violence are no longer confined to interpersonal relationships. They may emerge within organizational structures, digital ecosystems, commercial environments, political campaigns, foreign influence operations, and information systems operating at societal scale.

This development raises an important question:

Do existing legal frameworks provide adequate protection against contemporary forms of psychological violence and their long-term consequences – regardless of whether the perpetrator is domestic, foreign, commercial, or institutional?

This paper examines that question through a comparative analysis of European legal frameworks and proposes cognitive integrity as a potential emerging legal interest deserving greater protection.

1.1 Scope, Methodology and Conceptual Approach

This paper focuses primarily on psychological violence as a legal category.

However, psychological violence is also examined as a contributing factor to cognitive dependency, an emerging phenomenon that may progressively undermine cognitive integrity and, ultimately, cognitive sovereignty.

Methodology: This paper is based on a doctrinal legal analysis of European Union legislation, Council of Europe instruments, and selected national implementations. Primary sources include the Istanbul Convention, Directive (EU) 2024/1385, the Digital Services Act, the AI Act, the GDPR, GREVIO General Recommendation No. 1 (2021), and Council of the EU guidelines on cognitive warfare (2024). Comparative observations draw on country profiles published by the European Institute for Gender Equality (EIGE) and parliamentary questions concerning implementation deficits.



The objective of this analysis is not to establish cognitive sovereignty as a legal category. Rather, it is to examine whether existing legal developments suggest a gradual expansion of protected interests from physical integrity toward cognitive integrity and cognitive autonomy.

Three Interconnected Levels of Protection

This paper examines psychological violence at three interconnected levels, each corresponding to a distinct legal and political interest:

Level	Legal Interest	What Is Protected
Individual	Human right to cognitive integrity	The individual's capacity for autonomous judgment
Societal	Democratic resilience	Public discourse, civic participation, social trust
State	National security and sovereignty	The state's capacity to govern free from external coercion

These three levels are not separate. They are interconnected. The protection of the individual is the foundation. Without the individual, there is no legal interest and no protection. The protection of democracy and the state follow from the protection of individuals capable of independent judgment.

Actor-Neutral Approach

This paper adopts an actor-neutral approach to psychological violence. The focus is not on identifying specific states, institutions, or political actors. The focus is on **methods** – the techniques, systems and practices that impair autonomous judgment, regardless of who employs them.

Psychological violence may be perpetrated by:

- foreign state actors (through disinformation, cyber operations, cognitive warfare),
- commercial actors (through behavioural targeting, persuasive design, surveillance capitalism),
- domestic institutional actors (through strategic communication, narrative control, political manipulation),
- interpersonal actors (through coercive control, harassment, intimidation),
- or any combination thereof.

The legal question is not *who* is acting, but *what* they are doing and *whether* it impairs autonomous judgment in a legally significant way.

This actor-neutral approach serves three purposes:

First, it avoids the need to attribute psychological violence to specific states or institutions – a task that is often factually contested and politically charged.



Second, it ensures that the paper's conclusions apply universally. If a method is identified as psychologically violent, it does not matter whether the perpetrator is a foreign adversary, a commercial platform, a domestic agency, or a private individual.

Third, it preserves the focus on the **individual victim**. The right to cognitive integrity is not conditional on the identity of the perpetrator. Psychological violence harms the individual regardless of its source.

A detailed taxonomy of psychological violence mechanisms – including information manipulation, narrative coercion, attentional engineering, behavioural targeting, and algorithmic influence – is provided in the author's accompanying work *Good Morning, Europa: A Suicide Note – and a Survival Guide* (Hladnik, 2025). That work analyses specific techniques employed by various actors across political, commercial, and digital domains. This paper focuses on the legal framework and regulatory responses.

Four Core Concepts

The paper therefore explores four interconnected concepts:

Psychological Violence

The systematic use of communicative, behavioural, informational or environmental techniques that impair the ability of an individual or group to make free, informed and autonomous decisions, thereby undermining psychological integrity, cognitive autonomy or human dignity.

Cognitive Dependency

A condition in which beliefs, perceptions, preferences and decisions are predominantly shaped by external systems of influence rather than by autonomous evaluation and independent judgment.

Cognitive Integrity

The individual's right and capacity to maintain independent processes of perception, reflection, judgment and decision-making free from coercive, deceptive or systematically manipulative interference.

Cognitive Sovereignty

The continuous individual and collective effort to preserve autonomous judgment while navigating competing influences, narratives, interests and uncertainties.

At present, cognitive sovereignty should primarily be understood as a philosophical, ethical and societal concept rather than an established legal category.

Nevertheless, ongoing developments in data protection, platform regulation, artificial intelligence governance and the protection of mental autonomy suggest that some of its underlying principles may gradually find expression within future legal frameworks.



2. EXISTING LEGAL RECOGNITION OF PSYCHOLOGICAL VIOLENCE

2.1 The Istanbul Convention

The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) represents one of the most important milestones in the legal recognition of psychological violence.

The Convention requires signatory states to recognize and address forms of violence that do not necessarily involve physical injury.

Article 33 specifically addresses psychological violence and requires states to take legislative or other measures to criminalize intentional conduct seriously impairing a person's psychological integrity through coercion or threats.

The Convention recognizes:

- psychological violence,
- coercive behaviour,
- intimidation,
- harassment,
- controlling conduct,
- threats.

Its most important contribution lies in establishing a fundamental legal principle:

Violence does not require physical injury.

Psychological violence alone may constitute a violation of personal autonomy, dignity and integrity.

While the Istanbul Convention focuses primarily on domestic and interpersonal violence, its principles have been extended by GREVIO General Recommendation No. 1 (2021) to cover digital and technology-facilitated violence, including acts perpetrated by foreign actors operating across borders. The Convention does not distinguish between domestic and foreign perpetrators – its provisions apply to any actor within the jurisdiction of a State Party.

Nevertheless, the Convention remains largely focused on domestic and gender-based violence and does not address broader societal, political, commercial or digital forms of psychological influence, particularly those originating from foreign state actors.

2.1.1 GREVIO General Recommendation No. 1 (2021) – Digital Dimension of Psychological Violence



In October 2021, the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) adopted its first General Recommendation, dedicated to the digital dimension of violence against women.

This document explicitly applies the Istanbul Convention to acts of violence committed online or with the help of technology, including emerging technologies.

Key recognition: The digital dimension of violence against women is not a separate form of violence but rather an extension of existing forms – including psychological violence – amplified by technology.

The Recommendation identifies:

- online sexual harassment,
- online and technology-facilitated stalking,
- **the digital dimension of psychological violence.**

GREVIO calls on States Parties to:

- criminalize online threats, stalking and harassment,
- ensure that digital evidence is admissible in legal proceedings,
- require ICT companies and internet intermediaries to cooperate with law enforcement,
- provide training for law enforcement on investigating cyberviolence,
- establish easily accessible mechanisms for women to report abuse and obtain removal of harmful materials.

GREVIO's General Recommendation is particularly important because it recognizes that psychological violence in digital environments may be **systemic and technology-facilitated** rather than merely interpersonal. The Recommendation notes that the digital dimension exacerbates the harm caused by psychological violence due to the scale, speed and reach of online platforms – a characteristic that foreign actors may exploit to amplify their influence operations across borders.

This represents one of the first international legal recognitions that digital systems themselves may contribute to psychological violence, a principle that later found expression in the DSA and AI Act.

2.2 Directive (EU) 2024/1385 on Combating Violence Against Women and Domestic Violence

Directive (EU) 2024/1385 significantly expands the legal recognition of psychological violence within European Union law.

The Directive defines violence against women and domestic violence broadly and explicitly recognizes conduct causing or likely to cause:

- physical harm,
- sexual harm,



- **psychological violence,**
- economic harm.

One of its most important innovations is the explicit recognition of coercive control as a form of violence.

The Directive also addresses digitally mediated forms of abuse and requires Member States to criminalize:

- cyber stalking,
- cyber harassment,
- cyber flashing,
- non-consensual dissemination of intimate images,
- online incitement to violence or hatred.

This represents an important legal development because it acknowledges that psychological violence increasingly occurs through digital environments rather than exclusively through direct interpersonal interactions.

The Directive does not distinguish between domestic and foreign perpetrators. Its provisions apply to any actor, regardless of origin, who engages in the prohibited conduct within the jurisdiction of a Member State. Foreign actors operating from outside the EU may be prosecuted under national criminal laws implementing the Directive, subject to jurisdictional limitations. Universal jurisdiction – the principle that certain serious crimes can be prosecuted regardless of where they were committed – is generally not recognized for psychological violence under international law. However, where psychological violence accompanies other serious offences (e.g., torture, crimes against humanity, war crimes), universal jurisdiction may apply. In most cases, prosecution of foreign actors depends on traditional mechanisms such as extradition and mutual legal assistance treaties.

Implementation timeline: Member States are required to transpose the Directive into national legislation by **June 2027**.

The Directive reinforces a principle already emerging from the Istanbul Convention:

Psychological violence may be legally actionable even in the absence of physical injury.

Moreover, the Directive reflects growing recognition that digital technologies can facilitate, amplify and perpetuate psychological violence at unprecedented scale – a reality that foreign actors, commercial platforms and domestic institutions all exploit, albeit for different purposes.

2.3 Workplace Harassment and Mobbing

Most European legal systems recognize forms of workplace psychological violence through labor law, occupational safety regulations and anti-harassment frameworks.

Although terminology varies across jurisdictions, common legal concepts include:



- workplace harassment,
- mobbing,
- intimidation,
- humiliation,
- exclusion,
- hostile work environments,
- systematic psychological pressure.

These legal protections are based on the recognition that sustained psychological abuse can produce significant harm to mental health, dignity, professional development and overall well-being.

Workplace regulation therefore constitutes an important example of legal recognition of psychological violence beyond family relationships.

However, such protections remain confined to specific organizational contexts and generally do not address wider societal influence systems, whether domestic, commercial or foreign.

2.4 Consumer Protection Law

Consumer protection law provides another example of legal recognition that psychological mechanisms can influence human behavior.

European legislation prohibits:

- misleading advertising,
- deceptive commercial practices,
- hidden commercial influence,
- certain manipulative digital design practices (dark patterns),
- unfair behavioural targeting practices.

The legal rationale is that consumers should be able to make informed and autonomous decisions.

However, consumer protection law remains primarily concerned with economic harm and market fairness.

Its principal objective is not the protection of cognitive autonomy or psychological integrity as such.

Nevertheless, it establishes an important precedent:

Systematic manipulation of decision-making processes can justify legal intervention even in the absence of physical harm – a principle that applies equally to manipulation originating from commercial, domestic, or foreign actors.

2.5 General Data Protection Regulation (GDPR)



The General Data Protection Regulation (GDPR) represents one of the most significant legal developments relevant to the protection of psychological autonomy in the digital age.

Although GDPR is primarily understood as a data protection instrument, several of its provisions directly address practices capable of influencing human decision-making through profiling and automated processing.

Two provisions are particularly relevant.

Article 22 – Automated Individual Decision-Making

Article 22 grants individuals the right not to be subject to decisions based solely on automated processing where such decisions produce legal effects or similarly significant consequences.

This provision reflects a fundamental concern that individuals may be subjected to decisions affecting their lives without meaningful human oversight – a risk that applies whether the automated system is operated by a domestic company, a foreign platform, or a state actor.

Article 35 – Data Protection Impact Assessments

Article 35 requires organizations to conduct Data Protection Impact Assessments (DPIAs) whenever processing activities are likely to result in high risks to the rights and freedoms of natural persons.

Such assessments frequently involve profiling, behavioural prediction and large-scale data analytics.

Extraterritorial application: GDPR applies to any entity processing personal data of individuals in the EU, regardless of whether the entity is established inside or outside the EU (Article 3). This includes foreign state actors, commercial entities, and non-state groups operating from outside the EU. However, enforcement against foreign actors remains challenging and depends on international cooperation, mutual legal assistance, and the political will of third countries.

Although GDPR does not explicitly refer to psychological violence, it introduces important safeguards against forms of digital influence that may undermine autonomy through extensive behavioural profiling and automated decision-making.

GDPR therefore contributes to the gradual emergence of legal protections extending beyond privacy toward broader concerns related to individual autonomy and self-determination – regardless of the actor's origin.

2.6 Artificial Intelligence Act (AI Act) – Article 5 Prohibitions

Regulation (EU) 2024/1689, commonly known as the AI Act, introduces one of the strongest legal recognitions of manipulative influence currently found in European law.



The Regulation explicitly prohibits certain categories of artificial intelligence systems deemed incompatible with fundamental rights and democratic values.

Article 5(1)(a) prohibits AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques with the objective or effect of materially distorting a person's behavior in a manner that causes or is reasonably likely to cause significant harm.

Article 5(1)(b) prohibits AI systems that exploit vulnerabilities arising from age, disability or socio-economic circumstances with the objective or effect of materially distorting behavior in a manner causing or likely to cause significant harm.

Article 5(1)(c) prohibits AI systems for harmful social scoring – evaluating or classifying natural persons based on social behavior or predicted personal characteristics – leading to detrimental or unfavorable treatment.

Extraterritorial application: The AI Act's prohibitions apply to any provider placing an AI system on the EU market or putting it into service in the EU, regardless of whether the provider is established in the EU or abroad. Foreign actors deploying manipulative AI systems against EU citizens are subject to the same prohibitions as domestic actors. Enforcement against foreign actors, however, may face practical and jurisdictional obstacles.

The AI Act therefore **explicitly recognizes cognitive manipulation as a form of harm** – regardless of whether it causes physical or economic injury and regardless of whether the perpetrator is domestic, foreign, commercial, or institutional. This is an important precedent for recognizing psychological violence as a distinct legal category.

The significance of these prohibitions extends far beyond technical regulation.

For the first time, European law explicitly acknowledges that certain forms of cognitive manipulation may be unacceptable even in the absence of physical injury.

The AI Act therefore establishes an important legal precedent demonstrating that European lawmakers increasingly recognize the need to protect individuals not only from physical harm but also from manipulative interference with autonomous decision-making – a protection that must hold against all actors, foreign and domestic alike.

3. DIGITAL REGULATION AND SYSTEMIC PSYCHOLOGICAL RISKS

3.1 The Digital Services Act (DSA)

The Digital Services Act (DSA) represents a significant evolution in European regulatory thinking.



Unlike traditional criminal law, which focuses primarily on individual offenders and specific harmful acts, the DSA addresses systemic risks arising from the structure and operation of digital platforms.

This distinction is particularly important.

Psychological violence in digital environments often emerges not from a single identifiable actor but from the cumulative effects of recommendation systems, algorithmic amplification, engagement optimization and information architecture – whether operated by domestic platforms or foreign-controlled services.

The DSA therefore shifts attention from individual misconduct toward platform responsibility.

Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) are required to identify, assess and mitigate systemic risks related to:

- mental well-being,
- democratic discourse,
- electoral processes,
- public security,
- fundamental rights,
- dissemination of harmful content,
- violence based on gender.

This represents one of the first large-scale regulatory recognitions that digital systems themselves may contribute to psychological violence and democratic degradation – a risk that is magnified when platforms are controlled by foreign actors seeking to influence EU public opinion.

The DSA applies to all platforms offering services in the EU, regardless of their place of establishment. This includes platforms controlled by foreign state actors or entities. However, enforcement against foreign platforms may be complicated by jurisdictional and political constraints, including non-cooperation by third-country authorities.

3.2 Risk-Based Regulation

Articles 34 and 35 of the DSA establish a preventive regulatory model.

Platforms are required to:

- identify systemic risks,
- assess the likelihood and severity of harm,
- implement mitigation measures,
- evaluate the effectiveness of those measures,
- cooperate with regulatory authorities.

Potential mitigation measures include:



- algorithmic modifications,
- transparency obligations,
- reduction of harmful amplification,
- content labeling,
- deepfake identification,
- improved reporting mechanisms.

Unlike criminal law, which reacts after harm occurs, the DSA seeks to reduce the probability of harm before it reaches societal scale. This preventive approach is particularly valuable for addressing foreign influence operations, which often aim to shape public opinion gradually over time rather than through single identifiable events.

This preventive approach may provide a useful model for future regulation of broader forms of psychological violence.

Prior to the DSA, the Code of Practice on Disinformation (2022) established voluntary commitments for platforms to increase transparency, reduce manipulative advertising, and combat disinformation. The DSA has since made some of these commitments enforceable for Very Large Online Platforms (VLOPs), while the Code remains relevant for smaller platforms and as a benchmark for industry self-regulation.

3.3 Protection of Democratic Processes

The DSA explicitly recognizes risks affecting democratic discourse and electoral integrity.

This recognition is particularly significant because it acknowledges that information environments may influence not only individual well-being but also collective democratic decision-making.

Modern democracies increasingly depend on digital information systems.

Consequently, manipulation of these systems may affect:

- public opinion formation,
- electoral outcomes,
- civic participation,
- trust in institutions,
- social cohesion.

Foreign actors have been documented to exploit these vulnerabilities through disinformation campaigns, coordinated inauthentic behavior, and algorithmic manipulation. The DSA's risk-based framework is designed to address such threats regardless of their origin – domestic, foreign, commercial, or political.

The DSA therefore establishes an important legal connection between information environments and democratic resilience.



This connection closely parallels broader concerns regarding cognitive dependency and cognitive autonomy.

3.4 Artificial Intelligence Act (AI Act) – Extended Analysis

As introduced in section 2.6, the AI Act prohibits certain manipulative AI practices. The Act's broader framework also includes:

- **Conformity assessments** for high-risk AI systems,
- **Transparency obligations** for general-purpose AI,
- **Market surveillance** mechanisms,
- **Fines** up to €35 million or 7% of global turnover.

The AI Act's prohibitions on manipulative AI practices are particularly relevant to psychological violence because they do not require proof of physical or economic harm. Material distortion of behavior through subliminal or exploitative techniques is prohibited as such – regardless of whether the AI system is developed by a domestic company, a foreign state actor, or a commercial platform.

This represents a significant evolution in European legal thinking: **cognitive manipulation itself may be unlawful**, regardless of its consequences and regardless of the actor's identity.

Foreign actors deploying manipulative AI systems against EU citizens are subject to the same prohibitions as domestic actors, subject to the practical limitations of extraterritorial enforcement.

3.5 Cognitive Warfare, Hybrid Threats and Democratic Resilience

Recent European and transatlantic policy discussions increasingly address cognitive warfare, information warfare and hybrid threats.

The term "cognitive warfare" gained prominence in official discourse after German Defense Minister Christine Lambrecht used it in a NATO context in 2022, referring to hybrid operations targeting perceptions, emotions, and decision-making at the societal level. Since then, the concept has been adopted by NATO, the EU, and various national defense establishments.

Council of the EU Guidelines on Cognitive Warfare (4 October 2024)

On 4 October 2024, the Council of the EU (within the framework of the Working Party on Hybrid Threats) issued guidelines on cognitive warfare, defining it as:

"A coordinated, targeted and scientifically grounded effort to influence people's perceptions, emotions, decision-making and behavior at the individual and collective level."

The guidelines identify cognitive warfare as an emerging hybrid threat, distinct from traditional disinformation or psychological operations. They call for:

- protection of **cognitive security** as part of national security,



- improved media and information literacy,
- resilience-building at the societal level,
- cross-sectoral cooperation between defense, interior, digital affairs and education.

While these guidelines are not legally binding, they represent an important political signal and a foundation for future regulation. They explicitly link cognitive manipulation to national security, elevating the issue beyond individual victim protection.

Crucially, the guidelines do not identify specific adversaries. They describe methods and threats generically, recognizing that cognitive warfare techniques may be employed by any state or non-state actor seeking to influence EU societies.

Although these frameworks remain primarily strategic and security-oriented rather than legally binding, they reflect growing institutional recognition that influence operations may target:

- perception,
- emotions,
- beliefs,
- social trust,
- political behavior,
- collective decision-making.

Contemporary cognitive warfare strategies often seek to influence societies without direct military confrontation.

Their objective is frequently to shape how populations perceive reality and evaluate competing narratives.

The emergence of cognitive warfare as a recognized policy concern demonstrates that psychological influence is no longer viewed exclusively as an interpersonal phenomenon.

Instead, it is increasingly understood as a matter of national resilience, democratic stability and societal security – requiring protection at the individual, societal and state levels simultaneously.

While cognitive warfare frameworks should not be treated as legal authorities, they provide valuable evidence of the growing relevance of psychological influence within contemporary governance and security debates.

For a detailed analysis of cognitive warfare techniques, including the Integrity Initiative case study and the exploitation of nudging for political manipulation, see Tögel (2023), discussed in section 6.6 of this paper.

3.6 National Implementation: The Case of Slovenia (ZMed-1, 2025)

While this paper focuses primarily on European Union legislation, a brief examination of national implementation illustrates how legal frameworks operate in practice. Slovenia provides a useful example.



The Media Act (ZMed-1) – Adopted September 2025

On 3 September 2025, the Slovenian National Assembly adopted the **Media Act (ZMed-1)**, the first comprehensive reform of media legislation in over twenty years. The Act entered into force on 27 September 2025.

ZMed-1 implements the European Media Freedom Act (Regulation (EU) 2024/1083), which establishes common standards for media pluralism, editorial independence, and protection of journalists across the EU. The EMFA requires Member States to protect media from political interference, ensure transparent allocation of state advertising, and safeguard the independence of public service media.

Key provisions relevant to psychological violence and information pollution include:

Provision	Content	Relevance
Article 51	Prohibition of incitement to violence or hatred and incitement to terrorist acts	Applies to ALL forms of communication intended for the general public, including influencers
Article 52	Protection of minors	Additional safeguards against harmful content
Article 23	Disclosure of conflicts of interest	Transparency of ownership and financing
Article 3(4)	Editorial responsibility includes AI	Editorial responsibility extends to control over program content generated, partially generated, selected or arranged with the assistance of artificial intelligence
Mandatory AI labeling	Content generated with generative AI must be clearly labeled	Transparency and prevention of AI-driven manipulation
Media Registry ("Media Cadastre")	Public insight into media ownership structures and state advertising expenditures	Prevention of hidden concentration and opaque financing

Definitional scope (Article 2, paragraph 4):

"The provisions of this Act on disclosure of conflicts of interest (Article 23), prohibition of incitement to violence or hatred and incitement to terrorist acts (Article 51), protection of minors (Article 52) and advertising, sponsorship and product placement (Articles 55 to 62) apply to all forms of communication intended for the general public, which also includes the activity of influencers, regardless of whether they are considered media under this Act."

This means the Act **explicitly regulates forms of communication that are not traditional media** – including social media influencers – which is crucial for addressing information pollution in the digital space, whether originating from domestic or foreign sources.



Relevance to psychological violence: ZMed-1 addresses the communication dimension of psychological violence (incitement to hatred, harmful content targeting minors) but does not yet recognize cognitive dependency or cognitive sovereignty as distinct legal concepts.

AKOS as Digital Services Coordinator

The Agency for Communication Networks and Services of the Republic of Slovenia (AKOS) is the Slovenian national Digital Services Coordinator under the DSA. Recent activities relevant to psychological violence include:

- Support for the European Commission's investigation into X's use of AI tool Grok for generating manipulated sexually explicit images (February 2026)
- Investigation into Roblox platform regarding potential risks to minors (February 2026)
- Appointment of a Trusted Whistleblower working in the field of protection of minors

Regulatory gaps in Slovenia:

- No standalone criminal offence of psychological violence outside domestic violence context
- Stalking proposed but not yet enacted as separate offence
- No specific legislation on cognitive manipulation comparable to France or Spain
- Limited systematic data collection on psychological violence

The Slovenian example illustrates both the progress made (ZMed-1, AKOS as DSA coordinator) and the gaps that remain (no standalone psychological violence offence, no recognition of cognitive dependency).

4. COMPARATIVE ANALYSIS OF EXISTING LEGAL FRAMEWORKS

The legal instruments examined above reveal a gradual expansion in the recognition of psychological violence.

However, they differ substantially in their objectives, scope and regulatory mechanisms.

Framework	Protected Interest	Level Protection	of Applies to Foreign Actors?
Istanbul Convention	Psychological Integrity	Individual	Yes (within jurisdiction)
GREVIO Rec. No. 1 (2021)	General Digital Psychological Integrity	Individual Systemic	+ Yes
Directive (EU) 2024/1385	Psychological Integrity	Individual	Yes (subject to jurisdiction)
Labour Law / Anti-Harassment Law	Dignity and Mental Health	Organizational	Limited
Consumer Protection Law	Economic Autonomy	Commercial	Yes (if offering in EU)



Framework	Protected Interest	Level Protection	of Applies to Foreign Actors?
GDPR	Informational Determination	Self-Digital	Yes (extraterritorial, Art. 3)
Digital Services Act	Mental Well-being and Democratic Processes	Societal	Yes (regardless of establishment)
AI Act	Cognitive Autonomy and Human Agency	Digital	Yes (extraterritorial)
ZMed-1 (Slovenia)	Media Pluralism, Prohibition of Hate Speech	National	Applies to all content accessible in Slovenia

The comparison reveals an important trend.

The concept of protection gradually expands:

from bodily integrity,

to psychological integrity,

to informational self-determination,

and increasingly toward concerns related to cognitive autonomy.

At the same time, the legal instruments increasingly apply to foreign actors – through extraterritorial provisions (GDPR, AI Act), jurisdictional rules (Directive 2024/1385), or market-based mechanisms (DSA). Enforcement against foreign actors, however, remains a significant practical challenge.

The evolution is neither linear nor complete.

Nevertheless, it suggests the emergence of a broader legal interest centered on protecting the conditions necessary for autonomous judgment – regardless of whether the threat originates from domestic, foreign, commercial, or institutional actors.

4.1 Regulatory Overlaps and Dual Accountability

Contemporary forms of psychological violence increasingly operate across multiple regulatory domains simultaneously, often crossing borders in the process.

For example:

- cyber harassment may constitute both a criminal offense and a platform-related systemic risk,
- coordinated hate campaigns may trigger both criminal liability and regulatory intervention,



- manipulative recommendation systems may amplify conduct that is independently unlawful,
- behavioural targeting may intersect with data protection, consumer protection and platform regulation,
- foreign disinformation campaigns may involve platforms, advertisers, and state-sponsored actors.

As a result, contemporary legal systems increasingly employ a **dual accountability structure**.

Individual Accountability

Responsibility for direct acts of intimidation, harassment, coercion or manipulation – applicable to individuals regardless of nationality or residence, subject to jurisdictional rules.

Institutional Accountability

Responsibility for systems that enable, facilitate or amplify harmful conduct – applicable to platforms, AI providers, and other organizations regardless of their place of establishment if they offer services in the EU.

This dual model may become increasingly important as psychological influence shifts from interpersonal relationships toward complex technological and organizational systems – and as foreign actors exploit jurisdictional gaps to evade accountability.

5. REGULATORY GAPS

Despite substantial legal progress, important regulatory gaps remain.

The evolution of legal protections has been significant, yet current frameworks continue to address psychological violence through fragmented and sector-specific approaches.

The result is a growing discrepancy between contemporary mechanisms of influence and existing legal categories – a gap that foreign actors, commercial platforms, and domestic institutions may exploit.

5.1 Absence of a Unified Definition

One of the most significant limitations of current regulation is the absence of a unified definition of psychological violence applicable across societal domains and regardless of the actor's origin.

Existing legal definitions were developed within specific contexts such as:

- domestic violence,
- workplace harassment,
- discrimination,
- cybercrime,
- consumer protection.



As a result, legal recognition remains fragmented.

The same psychological mechanisms may be treated differently depending on the context in which they occur and depending on who employs them.

For example:

- intimidation within a family relationship may constitute a criminal offense,
- intimidation in the workplace may constitute harassment,
- intimidation in political communication may remain entirely lawful,
- intimidation through digital amplification may fall within platform regulation rather than criminal law,
- intimidation by foreign actors may fall outside any clear legal category.

This fragmentation creates conceptual inconsistency and regulatory uncertainty – and creates opportunities for actors to exploit gaps between legal categories.

5.1.1 Why Existing Definitions Are No Longer Sufficient

Traditional legal definitions of psychological violence were developed primarily in the context of domestic violence, workplace harassment and interpersonal relationships.

Contemporary societies increasingly experience forms of psychological influence that are:

- systemic rather than interpersonal,
- algorithmic rather than direct,
- persistent rather than episodic,
- collective rather than individual,
- commercial or political rather than personal,
- cross-border rather than local.

Existing legal definitions therefore capture only part of the phenomenon.

Modern influence systems increasingly operate through:

- digital platforms,
- behavioural targeting,
- algorithmic recommendation systems,
- large-scale political communication,
- commercial attention-extraction models,
- artificial intelligence systems,
- foreign disinformation networks.

Their effects may be cumulative and long-term rather than immediate and easily identifiable.

Consequently, legal frameworks developed for interpersonal abuse often struggle to address psychological influence operating at societal scale – whether originating from domestic commercial platforms or foreign state actors.



This creates a growing gap between traditional legal categories and contemporary mechanisms of influence.

5.2 Political and Ideological Manipulation

Current legal frameworks provide only limited tools for addressing psychological influence within political communication – whether domestic, foreign, or transnational.

Examples include:

- fear-based campaigns,
- systematic stigmatization,
- narrative coercion,
- emotional polarization,
- large-scale manipulation of public perception,
- foreign disinformation operations targeting electoral processes.

Such practices may significantly affect democratic deliberation while remaining outside existing legal categories.

The challenge is particularly complex because democratic societies must simultaneously protect:

- freedom of expression,
- political competition,
- open public debate,
- national security against foreign manipulation.

These observations apply across the political spectrum and should not be interpreted as targeting any specific ideology, political movement or institutional actor.

The concern is not the content of political views themselves but the systematic use of psychological techniques that may undermine autonomous judgment, informed consent or democratic deliberation – regardless of whether the techniques are employed by domestic political parties, commercial platforms, or foreign state actors.

5.3 Commercial Behavioural Manipulation

Commercial influence systems have evolved far beyond traditional advertising.

Modern digital environments increasingly rely upon:

- behavioural targeting,
- predictive analytics,
- attention engineering,
- persuasive design,
- addictive interface structures,
- algorithmic optimization of engagement.



These practices are often designed to influence behavior without requiring conscious reflection.

While consumer protection law addresses some forms of deception, current regulation remains largely focused on economic harm.

The broader psychological consequences of behavioural manipulation remain insufficiently addressed – whether the manipulator is a domestic corporation, a foreign-controlled platform, or an advertising network operating across borders.

This creates an important regulatory gap between consumer protection and cognitive autonomy.

5.4 Algorithmic Influence Systems

Recommendation systems increasingly shape:

- information exposure,
- social interactions,
- political engagement,
- consumer choices,
- public discourse.

Algorithms may influence decisions without explicit coercion.

They often operate through:

- personalization,
- selective amplification,
- reinforcement loops,
- attention optimization.

Although the DSA and AI Act represent important regulatory advances, many forms of algorithmic influence remain difficult to assess, monitor and regulate – particularly when algorithms are operated by foreign actors who may not cooperate with EU authorities.

The challenge becomes even greater when influence emerges from interactions among multiple systems rather than from a single identifiable actor, and when those systems are distributed across multiple jurisdictions.

5.5 Cognitive Dependency as a Regulatory Blind Spot

Existing legal frameworks recognize psychological violence primarily as discrete and identifiable injuries.

They do not recognize cognitive dependency.

Definition of Cognitive Dependency



Cognitive dependency may be defined as a chronic condition in which an individual's capacity for independent judgment, critical reflection and autonomous decision-making is progressively weakened by persistent systems of influence.

Unlike psychological violence, cognitive dependency does not necessarily require malicious intent.

It may emerge gradually through prolonged exposure to:

- informational environments,
- commercial influence systems,
- institutional narratives,
- algorithmic recommendation structures,
- technologically mediated decision-making processes,
- foreign disinformation campaigns,
- or any combination thereof.

Three Levels of Impact

Cognitive dependency operates at three interconnected levels, each corresponding to a distinct legal and political interest:

Level	Interest	Consequence of Cognitive Dependency
Individual	Human right to cognitive integrity	Loss of autonomous judgment; vulnerability to manipulation
Societal	Democratic resilience	Erosion of public discourse; polarization; loss of trust
State	National security and sovereignty	Vulnerability to foreign influence; reduced capacity for autonomous governance

The protection of the individual is the foundation. Without the individual, there is no legal interest and no protection. The protection of democracy and the state follows from the protection of individuals capable of independent judgment.

Foreign and External Actors

Cognitive dependency may be induced by foreign actors seeking to influence public opinion in another country, by commercial platforms optimizing for engagement, by domestic institutions shaping public discourse, or by any combination thereof. The mechanisms are often similar regardless of the actor.

For example, a foreign state-sponsored disinformation campaign, a domestic political party's narrative strategy, and a commercial platform's engagement algorithm may all employ repetition, emotional targeting, and selective information exposure. The harm to the individual – the gradual erosion of autonomous judgment – is the same regardless of the source.

Mechanisms and Taxonomy



A detailed taxonomy of mechanisms inducing cognitive dependency – including information overload, narrative repetition, emotional polarization, algorithmic echo chambers, attentional capture, and behavioural targeting – is provided in the author's accompanying work *Good Morning, Europa: A Suicide Note – and a Survival Guide* (Hladnik, 2025, Chapters 3–5). That work analyzes specific techniques employed by various actors across political, commercial, and digital domains. This paper focuses on legal consequences rather than mechanism taxonomy.

Comparative Characteristics

Traditional violence	Psychological	Cognitive Dependency
Episodic		Chronic
Specific incident		Long-term process
Identifiable perpetrator		Diffuse influence systems (domestic, foreign, commercial)
Recognizable victimization		Often invisible to the individual
Individual responsibility		Systemic causation
Existing legal remedies		Limited or absent remedies

This represents one of the most significant blind spots in contemporary regulation.

Individuals may lose substantial cognitive autonomy without any single act reaching the threshold of unlawful conduct. Foreign actors may exploit this gap. Commercial platforms may benefit from it. Democratic societies may suffer from it.

The legal response must therefore be method-focused and actor-neutral, while recognizing that enforcement against foreign actors requires international cooperation and political will.

5.6 Asymmetric Regulation: Public vs. Private vs. Foreign Actors

A notable feature of existing European legal frameworks is their **asymmetric application**.

Private actors (digital platforms, AI providers, media companies, commercial advertisers) are subject to extensive regulation under the DSA, AI Act, GDPR, and consumer protection law. Foreign actors are increasingly regulated through sanctions, election integrity measures, and diplomatic instruments, though enforcement remains challenging.

Public institutions – including the European Commission, the European Parliament, national governments, and their agencies – are not subject to equivalent transparency and accountability standards when engaging in public communication, strategic communication, or public diplomacy.

This asymmetry raises a question of consistency. If psychological violence is defined by the **method** (e.g., manipulative targeting, behavioural engineering, narrative coercion), should the same standards apply regardless of whether the actor is private, foreign, or public?



The answer is not self-evident. Democratic institutions have a legitimate mandate to inform and persuade citizens. Public information campaigns, educational initiatives, and public health messaging are essential functions of governance. However, when public communication employs methods that would be prohibited for private actors (e.g., non-transparent behavioural targeting, subliminal techniques, exploitative design), the legitimacy of such methods becomes questionable.

This paper does not allege that European institutions engage in psychological violence. It merely notes that existing legal frameworks do not address this question. The same methods that are regulated when used by private or foreign actors remain unexamined when used by public institutions. Future research and policy debate should consider whether consistency requires extending transparency and accountability standards to public communication.

This observation applies across the political spectrum. It is not directed at any specific institution, government, or political orientation. It is a structural observation about the architecture of European regulation.

The Foreign Actor Gap

Foreign actors present a distinct challenge. While EU law increasingly applies extraterritorially (GDPR Article 3, AI Act extraterritorial scope, DSA application to non-EU establishments), enforcement against foreign actors depends on:

- international cooperation,
- mutual legal assistance treaties,
- extradition arrangements,
- political will of third countries,
- the willingness of platforms to comply with EU orders.

When foreign actors operate from jurisdictions that do not cooperate with EU authorities, legal remedies may be unavailable. This gap cannot be closed by EU law alone; it requires diplomatic and geopolitical strategies beyond the scope of this paper.

Existing mechanisms for cross-border enforcement include mutual legal assistance treaties (MLATs), extradition agreements, the European Investigation Order (EIO) for cooperation within the EU, and coordination through Eurojust and Europol. However, these mechanisms are often slow, politically sensitive, and depend on the goodwill of third countries. For foreign actors operating from jurisdictions that do not recognize EU legal authority or refuse to cooperate, enforcement remains a significant practical obstacle.

6. THEORETICAL CONTEXT AND INTELLECTUAL FOUNDATIONS

6.1 Propaganda, Public Opinion and Manufactured Consent

Hannah Arendt (1906–1975)

Key concept: Totalitarianism, propaganda and the destruction of factual reality.



Arendt argued that totalitarian regimes do not merely suppress dissent but actively destroy the capacity for independent judgment by blurring the distinction between fact and fiction, truth and falsehood. Her analysis of propaganda as a tool for reshaping reality is directly relevant to contemporary concerns about information manipulation – whether employed by foreign adversaries, domestic regimes, or commercial platforms.

Connection to this paper: Arendt's work illuminates how systematic information manipulation can erode the conditions necessary for autonomous judgment – a process closely related to what this paper terms cognitive dependency. Her analysis applies regardless of which actor employs the techniques.

Noam Chomsky (b. 1928) and Edward Herman (1925–2017)

Key concept: Manufacturing Consent (1988).

Chomsky and Herman proposed a "propaganda model" of media in which structural filters (ownership, advertising, sourcing, flak, anti-communist ideology) systematically shape news content. Their work demonstrates how institutional arrangements can produce conformity without explicit coercion – a phenomenon observable in both domestic and foreign media systems.

Connection to this paper: The propaganda model illustrates how systemic, institutional factors can shape public perception – an early formulation of what this paper calls systemic psychological influence. The model is actor-neutral: similar structural filters operate in different political and commercial systems.

6.2 Psychological Mechanisms of Influence

Daniel Kahneman (b. 1934)

Key concept: System 1 and System 2 thinking (Thinking, Fast and Slow, 2011).

Kahneman demonstrated that human cognition operates through two systems: System 1 (fast, intuitive, automatic) and System 2 (slow, deliberative, analytical). System 1 is highly susceptible to cognitive biases and framing effects.

Connection to this paper: Kahneman's work explains why manipulation works. Influence systems often target System 1 processing, bypassing deliberative reasoning – a vulnerability exploited by commercial advertisers, political campaigns, and foreign disinformation operations alike.

Robert Cialdini (b. 1945)

Key concept: Principles of persuasion (authority, social proof, reciprocity, scarcity, liking, consistency).

Cialdini identified psychological mechanisms that reliably influence human behavior, often without conscious awareness.



Connection to this paper: These mechanisms are systematically exploited by commercial and political actors across all jurisdictions. Understanding them is essential for designing protective legal frameworks that are actor-neutral.

Mattias Desmet (b. 1970)

Key concept: Mass formation.

Desmet has analyzed how collective psychological processes can lead to shared beliefs and behaviors without rational foundation. His work explores how fear, uncertainty and social cohesion can produce mass psychological phenomena.

Connection to this paper: Desmet's analysis of collective psychological processes is relevant to understanding societal-level cognitive dependency, regardless of which actors trigger the process.

6.3 Digital Influence and Behavioural Engineering

Shoshana Zuboff (b. 1951)

Key concept: Surveillance capitalism (The Age of Surveillance Capitalism, 2019).

Zuboff argues that digital platforms have developed a new economic logic based on the extraction and prediction of human behavior. Behavioural data is used not only to target advertising but to modify behavior itself.

Connection to this paper: Surveillance capitalism describes the commercial production of behavioural dependency – a structural driver of cognitive dependency that operates across borders, involving both domestic and foreign-controlled platforms.

Jaron Lanier (b. 1960)

Key concept: Behavior modification business models.

Lanier has argued that social media platforms are not neutral tools but behavior modification engines designed to maximize engagement through psychological manipulation.

Connection to this paper: Lanier's critique identifies the commercial incentives that drive algorithmic influence systems – incentives that exist regardless of whether the platform is headquartered in the EU, the United States, or elsewhere.

Cass Sunstein (b. 1954)

Key concept: Nudging and choice architecture (Nudge, 2008, with Richard Thaler).

Sunstein has explored how the design of choice environments influences decision-making without restricting options. While nudging can be used for benign purposes (e.g., encouraging retirement savings), it can also be exploited for manipulation.



Connection to this paper: Sunstein's work illuminates the boundary between legitimate guidance and manipulative interference with autonomy – a boundary that must be defined in actor-neutral terms.

6.4 Power, Knowledge and Social Control

Michel Foucault (1926–1984)

Key concept: Disciplinary power and normalization.

Foucault analyzed how modern societies exercise power not primarily through coercion but through normalization – shaping what is considered normal, rational and desirable. Institutions (prisons, schools, hospitals, asylums) produce conformity through surveillance, classification and normalization.

Connection to this paper: Foucault's analysis of disciplinary power provides a framework for understanding institutional and societal influence systems that operate without explicit violence – applicable to both democratic and non-democratic contexts.

6.5 Contemporary Discussions of Cognitive Sovereignty

Mario Brcic (2025)

Key concept: Cognitive sovereignty in the age of AI.

Brcic defines cognitive sovereignty as *"the ability of individuals, groups, and nations to maintain autonomous thought and preserve identity in the age of powerful AI systems, especially those that hold their deep personal memory."*

He introduces concepts including Network Effect 2.0 (platform value grows with depth of personalized memory rather than user count), memory lock-in (users become cognitively dependent on AI assistants; switching is described as "cognitive amputation"), and AI colonialism (technologically advanced states or corporations dominate weaker markets by shaping cognitive patterns).

Connection to this paper: Brcic's work is the most direct theoretical precursor to this paper's concept of cognitive sovereignty. His analysis of memory lock-in is closely related to cognitive dependency and applies regardless of whether the AI provider is domestic or foreign.

Christian R. Klein (2025)

Key concept: Sovereignty Trap.

Klein describes a psychological mechanism where the authoritative competence of AI systems tempts users to cede their own intellectual judgment, mistaking access to information for genuine ability. He writes of the "hollowed mind" – a condition in which access to AI substitutes for genuine understanding.



Connection to this paper: The sovereignty trap is a specific mechanism contributing to cognitive dependency. Klein's analysis complements Brcic's focus on memory with a focus on judgment.

Gargi Tripathi and Lipi Saxena (2025)

Key concept: Epistemic colonization (The Managed Mind).

Tripathi and Saxena argue that mechanisms of power (from algorithms to institutional norms) operate within the citizen's own consciousness. They call for a new form of social contract that protects the integrity of the psyche. Their work connects cognitive sovereignty to political theory, arguing that classical definitions of freedom (absence of external interference) are no longer sufficient.

Connection to this paper: Epistemic colonization describes a process closely related to cognitive dependency. Tripathi and Saxena provide a political-philosophical foundation for the legal arguments developed in this paper.

Nita Farahany (2023)

Key concept: Cognitive liberty / Right to think freely (*The Battle for Your Brain*, 2023).

Farahany, a Duke University law professor, argues that emerging neurotechnologies (wearable brain sensors, neural implants, brain-computer interfaces, emotion detection algorithms) threaten **cognitive liberty** – the right to self-determination over one's own brain and mental processes.

Key concepts introduced by Farahany include:

Concept	Description
Cognitive liberty	The right to control one's own conscious and unconscious mental processes
Mental privacy	Protection against unauthorized access to brain data
Freedom from mind reading	Protection against technologies that claim to decode mental content
Freedom from brain manipulation	Protection against technologies that directly alter brain function

Connection to this paper: Farahany's concept of cognitive liberty is closely related to what this paper terms cognitive integrity. While Farahany focuses on neurotechnology (direct brain intervention), this paper focuses on psychological violence and influence systems (behavioural, informational and algorithmic manipulation). The two are complementary: neurotechnology threatens cognitive integrity from the *inside*, while influence systems threaten it from the *outside*. Both point toward the same conclusion: legal systems must expand protection to include mental autonomy and cognitive integrity, regardless of whether the threat originates from domestic medical technology, foreign surveillance, or commercial platforms.



6.6 Jonas Tögel (2023) – Cognitive Warfare

Jonas Tögel (active 2023–2025)

Key concept: Cognitive warfare (Kognitive Kriegsführung).

Tögel is a German American studies scholar and propaganda researcher at the University of Regensburg. His 2023 book *Kognitive Kriegsführung. Neueste Manipulationstechniken als Waffengattung der NATO* argues that NATO has been developing cognitive warfare since 2020, described as "the most advanced form of manipulation" with the goal of "hacking human thoughts like computers."

Tögel analyzes concrete cases including the Integrity Initiative (a British organization funded by the Foreign Office, MI6, GCHQ, the US State Department, Facebook, the British military and NATO) which conducted anti-Russian propaganda campaigns across Europe. He also examines how "nudging" (Thaler & Sunstein, 2008) can be exploited for political manipulation.

Connection to this paper: Tögel provides the most detailed analysis of psychological manipulation as systematic state practice. His work connects cognitive warfare to intelligence agencies, think tanks and media manipulation – precisely the "soft power" and "systematic manipulation" dimensions identified in the expanded definition of cognitive dependency. While Tögel focuses on NATO and Western actors, the mechanisms he describes are generalizable and may be employed by any state or non-state actor.

6.7 Synthesis and Original Contribution

The common thread across these theoretical contributions – from Arendt to Tögel, from Farahany to Brcic – is the recognition that psychological violence is not confined by borders.

Foreign actors, commercial platforms, domestic institutions and interpersonal perpetrators may employ similar methods. The mechanisms of influence – repetition, emotional targeting, selective exposure, algorithmic manipulation, behavioural engineering, narrative coercion – are universal. The harm to the individual – the gradual erosion of autonomous judgment – is the same regardless of the source.

The concept of **cognitive dependency** proposed in this paper synthesizes these observations into a common analytical framework. It suggests that persistent exposure to systems of influence may gradually weaken autonomous judgment and contribute to the erosion of cognitive integrity – whether those systems are operated by foreign adversaries, domestic institutions, or commercial platforms.

From this perspective, **cognitive sovereignty** should be understood not as freedom from influence, but as the continuous effort of individuals and societies to preserve independent judgment despite competing pressures, narratives and interests – and despite the fact that influence may originate from multiple directions simultaneously.

Original contribution of this paper: While existing literature has identified mechanisms of manipulation (Tögel), described cognitive sovereignty (Brcic), analyzed the sovereignty trap



(Klein), theorized epistemic colonization (Tripathi & Saxena), and warned of neurotechnological threats (Farahany), no previous work has:

1. Synthesized these observations into a unified legal framework applicable across domestic, foreign, commercial and institutional actors,
2. Proposed cognitive dependency as a distinct regulatory blind spot,
3. Traced the evolution of European law from physical integrity toward cognitive integrity,
4. Developed operational definitions suitable for legal application that are actor-neutral,
5. Explicitly addressed the asymmetric regulation of public vs. private vs. foreign actors.

This paper therefore contributes to the emerging interdisciplinary field of cognitive security and cognitive sovereignty by providing a legal-theoretical foundation for future regulatory development that protects individuals, democracies and states alike – regardless of where the threat originates.

A detailed taxonomy of specific mechanisms inducing cognitive dependency – including information overload, narrative repetition, emotional polarization, algorithmic echo chambers, attentional capture, and behavioural targeting – is provided in the author's accompanying work *Good Morning, Europa: A Suicide Note – and a Survival Guide* (Hladnik, 2025, Chapters 3–5). That work analyzes specific techniques employed by various actors across political, commercial, and digital domains, with detailed case studies. This paper focuses on legal consequences rather than mechanism taxonomy.

7. OPERATIONAL DEFINITION OF PSYCHOLOGICAL VIOLENCE

A major obstacle to coherent regulation is the absence of a general definition applicable across societal domains and across actor types (domestic, foreign, commercial, institutional).

For analytical and regulatory purposes, psychological violence may be defined as:

Psychological violence is the systematic use of communicative, behavioural, informational or environmental techniques that impair the ability of an individual or group to make free, informed and autonomous decisions, thereby violating psychological integrity, cognitive autonomy or human dignity, with the intention of obtaining benefits for the perpetrator or a third party.

This definition extends beyond traditional interpersonal abuse while remaining consistent with existing legal principles concerning dignity, autonomy and psychological integrity. It is **actor-neutral**: it does not distinguish between perpetrators based on their identity, origin, or affiliation.

The role of intent (mens rea): The inclusion of intent is essential for distinguishing criminal psychological violence from lawful influence. In democratic societies, many forms of influence – education, healthcare, parenting, public health campaigns, political persuasion – may temporarily reduce autonomy but are legitimate because their intent is to benefit the target or society. Psychological violence, by contrast, requires intent to benefit the perpetrator or a third party at the expense of the target's autonomy.



Psychological violence may include, but is not limited to:

- coercive control,
- intimidation,
- humiliation,
- stigmatization,
- emotional blackmail,
- gaslighting,
- isolation,
- information manipulation,
- narrative coercion,
- exploitation of cognitive vulnerabilities,
- manipulative behavioral targeting,
- non-transparent algorithmic influence.

The defining characteristic is not physical injury. The defining characteristic is the systematic reduction of autonomous judgment and decision-making capacity **for the benefit of another**.

What is NOT psychological violence – boundary clarification

Not every form of influence constitutes psychological violence. The following remain legitimate and protected in democratic societies:

- ordinary political debate and persuasion (intent: democratic competition, transparency)
- academic criticism and intellectual disagreement (intent: pursuit of truth)
- journalistic reporting (even when critical or uncomfortable) (intent: public information)
- commercial advertising (within existing consumer protection limits) (intent: profit, but regulated)
- social persuasion and informal influence among individuals (intent: mutual benefit)
- education and teaching (including authoritative instruction) (intent: student development)
- advocacy and activism (intent: social change, transparency)
- satire and parody (intent: commentary, entertainment)

The boundary between legitimate influence and psychological violence is crossed when influence becomes **systematic, opaque, asymmetrical and impairing** – that is, when it significantly reduces the target's capacity for autonomous judgment without their informed consent or awareness, **and when the intent is to benefit the perpetrator or a third party rather than the target**. This boundary applies equally to all actors: domestic, foreign, commercial, and institutional.

8. TOWARDS A NEW LEGAL PARADIGM

The evolution of European law suggests the emergence of a broader principle:



Protection of Cognitive Integrity

Traditionally, legal protection focused on:

- life,
- bodily integrity,
- property.

Modern constitutional democracies subsequently expanded protection to include:

- dignity,
- equality,
- privacy,
- informational self-determination.

Contemporary technological and geopolitical developments raise a new question:

Should legal systems also protect the conditions necessary for autonomous thought and judgment – regardless of whether the threat comes from domestic commercial platforms, foreign state actors, or domestic institutions?

This question becomes increasingly important as influence systems become more sophisticated, personalized and pervasive, and as foreign actors develop cognitive warfare capabilities targeting EU societies.

8.1 Evolution of Protected Legal Interests

Historical Phase	Primary Protected Interest
Classical Criminal Law	Life and Bodily Integrity
Modern Constitutional Law	Human Dignity
Information Age	Privacy and Informational Self-Determination
Emerging Digital Society	Cognitive Integrity

The historical development of law demonstrates a gradual expansion of protected human interests.

Initially, legal systems focused primarily on protecting life and bodily integrity.

Constitutional democracies later expanded protection to include dignity, equality and fundamental freedoms.

The information age introduced privacy and informational self-determination as essential protected interests.

The rise of digital influence systems, behavioural technologies, artificial intelligence, and foreign cognitive warfare operations now raises the question whether cognitive integrity may represent the next stage in this evolutionary process.



8.2 Cognitive Integrity as a Protected Legal Interest

Cognitive integrity may be understood as the individual's right and capacity to maintain independent processes of perception, reflection, judgment and decision-making free from coercive, deceptive or systematically manipulative interference.

As bodily integrity protects the body, cognitive integrity protects the processes through which individuals understand reality and make decisions.

The growing recognition of:

- coercive control,
- systemic digital risks,
- manipulative AI systems,
- behavioural targeting,
- the digital dimension of psychological violence (GREVIO, 2021),
- foreign cognitive warfare (Council of the EU, 2024),

suggests that elements of such protection are already emerging within European law.

Concrete examples of what cognitive integrity protection could mean in practice:

- **Right to cognitive rest:** Protection from algorithmic systems designed to capture and hold attention beyond reasonable limits – applicable to domestic and foreign platforms alike.
- **Right to transparency:** Individuals have the right to know when and how their behavior is being targeted by manipulative design, regardless of whether the manipulator is a domestic corporation or a foreign state actor.
- **Right to meaningful choice:** Choice architectures must not systematically deceive or coerce – a standard that applies to all actors operating within EU jurisdiction.
- **Right to disconnection:** The ability to opt out of behavioural tracking and algorithmic recommendation systems without losing access to essential services.

8.3 Cognitive Sovereignty as a Normative Objective

Cognitive sovereignty should currently be understood primarily as a philosophical, ethical and societal concept rather than an established legal category.

It refers to the continuous individual and collective effort to preserve autonomous judgment while navigating competing influences, narratives, interests and uncertainties – whether those influences originate from domestic commercial platforms, foreign disinformation campaigns, or domestic public institutions.

Nevertheless, ongoing developments in data protection, platform regulation, artificial intelligence governance and the protection of mental autonomy suggest that some of its underlying principles may gradually find expression within future legal frameworks.

9. RISKS OF OVERREGULATION



Recognition of psychological violence must not become a justification for censorship or ideological control.

Democratic societies must preserve:

- freedom of expression,
- political disagreement,
- intellectual pluralism,
- academic freedom,
- open democratic debate.

Concrete example of overregulation risk: A law prohibiting "information manipulation" could, if poorly drafted, be used by incumbent governments to suppress legitimate political opposition under the guise of protecting citizens from psychological violence. This risk exists regardless of whether the government is acting in good faith. It is particularly acute when laws are applied asymmetrically – for example, when used against political opponents but not against government-aligned actors, or when used against foreign critics but not against domestic institutions.

Future regulation should therefore focus primarily on:

- transparency,
- accountability,
- demonstrable harm,
- protection of autonomy,

rather than ideological conformity or restrictions on legitimate expression.

The objective is not protection from ideas.

The objective is protection from systematic practices that undermine the capacity for independent judgment – regardless of who employs those practices.

10. FUNDAMENTAL RIGHTS DIMENSION

The legal regulation of psychological violence cannot be examined solely through the lens of criminal law, labor law or digital regulation.

It must also be understood within the broader framework of fundamental rights and constitutional protections.

Several fundamental rights recognized in European and international legal instruments are directly relevant to the protection of psychological integrity and cognitive autonomy – and apply regardless of whether the threat originates from domestic or foreign actors.

10.1 Human Dignity



Human dignity occupies a central position within European constitutional traditions.

Article 1 of the Charter of Fundamental Rights of the European Union states:

Human dignity is inviolable. It must be respected and protected.

Psychological violence may undermine dignity by impairing an individual's capacity to exercise autonomous judgment, maintain personal integrity and participate freely in social and democratic life.

The protection of dignity therefore provides an important normative foundation for legal responses to psychological violence – a foundation that applies equally to threats originating from domestic institutions, foreign actors, and commercial platforms.

10.2 Integrity of the Person

Article 3 of the Charter guarantees the right to respect for the integrity of the person.

Historically, this protection was interpreted primarily in relation to physical and biomedical interventions.

However, technological developments increasingly raise questions concerning psychological and cognitive integrity.

The growing capacity to influence perception, beliefs and behavior through digital systems suggests that integrity may require broader interpretation in contemporary societies – including protection against manipulation regardless of the actor's origin.

10.3 Freedom of Thought, Conscience and Opinion

Article 10 of the Charter and Article 9 of the European Convention on Human Rights protect freedom of thought, conscience and religion.

These protections recognize the importance of maintaining independent intellectual processes free from coercion.

Although traditional legal interpretations focus on state interference, contemporary influence systems may create new challenges through:

- algorithmic persuasion,
- behavioural targeting,
- large-scale information manipulation,
- exploitative AI systems,
- foreign cognitive warfare.

The preservation of meaningful freedom of thought may therefore require renewed attention to the conditions under which opinions are formed – and to the actors, foreign or domestic, that may interfere with those conditions.



European Court of Human Rights jurisprudence: The ECtHR has increasingly recognized that Article 8 ECHR (right to private and family life) protects personal autonomy and psychological integrity. In cases such as *S. and Marper v. United Kingdom* (2008), the Court held that the retention of personal data affects the right to respect for private life. More recently, the Court has acknowledged that digital surveillance and data processing may interfere with personal autonomy. While no ECtHR case has yet recognized "cognitive integrity" as a distinct right, the trajectory of case law suggests openness to expanding protection in response to technological developments – regardless of whether the threat originates from domestic or foreign sources.

10.4 Privacy and Personal Autonomy

The European Court of Human Rights has repeatedly interpreted Article 8 ECHR as protecting not only privacy but also personal autonomy and psychological integrity.

Case law increasingly recognizes that respect for private life includes protection of an individual's capacity to develop personal identity and make autonomous life choices.

This jurisprudence provides an important foundation for future discussions concerning cognitive integrity – a foundation that applies across actor types.

10.5 Informational Self-Determination

European legal systems increasingly recognize that control over personal information is essential for individual autonomy.

GDPR reflects this principle through rights related to:

- transparency,
- consent,
- access,
- rectification,
- profiling,
- automated decision-making.

Informational self-determination represents an important step toward broader protection of cognitive autonomy because information environments significantly influence perception and decision-making – and because foreign actors increasingly exploit personal data for influence operations.

11. REGULATORY PRINCIPLES FOR FUTURE DEVELOPMENT

Any future legal framework addressing psychological violence must carefully balance protection against harm with the preservation of democratic freedoms – and must apply consistently across actor types.



Several principles should guide future regulatory development.

11.1 Necessity

Legal intervention should occur only where necessary to protect significant interests.

Not every form of influence justifies regulation.

Democratic societies necessarily involve persuasion, advocacy, political competition, education and public debate.

Regulation should therefore focus on practices that create substantial risks to autonomy, dignity or cognitive integrity – regardless of whether those practices are employed by domestic, foreign, commercial, or institutional actors.

Concrete example: A social media platform's use of infinite scroll to maximize engagement may create risks of attentional dependency, but banning infinite scroll might not be necessary if transparency and user control measures (e.g., default timers, easy opt-out) achieve the same protective goal with less restriction on platform design – and such measures should apply equally to domestic and foreign platforms.

11.2 Proportionality

Measures adopted to address psychological violence must remain proportionate to the harms involved.

Excessive regulation may itself threaten democratic freedoms.

The principle of proportionality therefore requires balancing:

- protection of autonomy,
- freedom of expression,
- democratic participation,
- open public discourse.

Concrete example: Prohibiting all political advertising would be a disproportionate response to the risk of manipulative political messaging – whether domestic or foreign. Requiring transparency (disclosure of funding, targeting criteria, and estimated audience size) is more proportionate and less restrictive.

11.3 Transparency

Transparency represents one of the least restrictive and most effective regulatory responses.

Examples include:

- transparency of political advertising (including foreign funding),
- transparency of algorithmic systems,



- transparency of behavioural targeting,
- transparency of AI-generated content,
- transparency of institutional influence campaigns,
- transparency of foreign state-sponsored content.

Transparency enhances autonomy without restricting legitimate communication – and applies equally to domestic and foreign actors.

11.4 Accountability

Organizations exercising significant influence over public perception should be accountable for foreseeable harms resulting from their systems and practices.

This principle may apply to:

- digital platforms (domestic and foreign),
- AI providers (domestic and foreign),
- public institutions,
- commercial actors,
- political organizations,
- foreign state-controlled media operating in the EU.

Accountability does not imply censorship.

Rather, it promotes responsible exercise of influence – and ensures that foreign actors operating in the EU are subject to the same standards as domestic actors.

11.5 Democratic Oversight

Given the complexity of modern influence systems, democratic oversight mechanisms are essential.

Such mechanisms may include:

- independent regulators,
- parliamentary oversight,
- judicial review,
- transparency reporting,
- public audits.

Oversight helps ensure that regulatory responses remain compatible with democratic values – and that they are applied consistently across actor types, without political favoritism or selective enforcement.

12. DEMOCRATIC DIMENSION



The significance of psychological violence extends beyond individual harm.

Democratic governance presupposes citizens capable of independent judgment.

Public debate, electoral competition and democratic participation all depend upon the existence of individuals who can evaluate information, consider alternatives and make autonomous decisions.

When psychological violence and cognitive dependency become systemic – whether induced by domestic commercial platforms, foreign disinformation campaigns, or domestic institutional narratives – democratic processes themselves may be affected.

Potential consequences include:

- reduced quality of public deliberation,
- increased polarization,
- declining institutional trust,
- weakened democratic participation,
- diminished capacity for collective problem-solving,
- vulnerability to foreign manipulation of electoral processes.

The protection of cognitive integrity is therefore not only an individual concern.

It is also a prerequisite for democratic resilience – and, at the state level, for national security and sovereignty.

Democratic societies depend not merely on formal institutions but on citizens capable of exercising meaningful judgment. When that capacity is systematically eroded, democracy itself is threatened – regardless of whether the erosion is caused by domestic commercial platforms, foreign state actors, or domestic institutions.

Comparative observation: Different democratic systems have adopted different approaches to these challenges. Some (e.g., Germany with its Network Enforcement Act) have emphasized rapid removal of harmful content. Others (e.g., France with its comprehensive approach to psychological violence) have emphasized criminal law responses. Still others (e.g., the EU through the DSA) have emphasized systemic platform accountability. No single model has proven definitively superior, suggesting that regulatory approaches must be adapted to national legal cultures and political contexts – while ensuring consistent protection against foreign manipulation.

13. LIMITATIONS

Several limitations should be acknowledged.

First, not all influence constitutes psychological violence.

Human societies depend upon communication, persuasion, education, advocacy and public debate.



Attempts to eliminate influence altogether would be both impossible and undesirable.

Second, psychological violence may be difficult to distinguish from legitimate influence in certain contexts.

Clear criteria are therefore necessary to avoid arbitrary interpretation – and must be applied consistently across actor types.

Third, cognitive dependency remains an emerging concept rather than a fully established legal category.

Further interdisciplinary research is needed to clarify its causes, manifestations and potential legal implications.

Open questions for further research:

- How can cognitive dependency be measured empirically?
- What threshold distinguishes legitimate influence from pathological cognitive dependency?
- Can cognitive dependency be reversed, and if so, through what interventions?
- How do different regulatory models (criminal law, platform regulation, consumer protection) interact in addressing cognitive dependency?
- What is the relationship between individual cognitive dependency and collective epistemic dysfunction?
- How can enforcement against foreign actors be improved without compromising international relations?
- Should public institutions be subject to the same transparency standards as private and foreign actors?

Fourth, future regulatory responses must avoid becoming instruments of censorship or ideological control.

The protection of autonomy must not undermine the freedoms upon which democratic societies depend.

The challenge is therefore not to suppress disagreement but to identify and address practices that substantially impair autonomous judgment – regardless of who employs them.

Fifth, the question of asymmetric application:

This paper has analyzed European legal frameworks as they are formally written. It has not examined whether these frameworks are applied asymmetrically – for example, whether public institutions are subject to the same transparency and accountability standards as private or foreign actors, or whether politically engaged individuals (journalists, activists, opposition politicians) receive greater protection in practice than non-engaged citizens. These empirical questions lie beyond the scope of this doctrinal legal analysis but deserve investigation.

Sixth, the foreign actor enforcement gap:



While EU law increasingly applies extraterritorially, enforcement against foreign actors depends on international cooperation, mutual legal assistance, and political will. When foreign actors operate from jurisdictions that do not cooperate, legal remedies may be unavailable. This gap cannot be closed by EU law alone.

Seventh, the actor-neutral limitation:

This paper adopts an actor-neutral approach, focusing on methods rather than perpetrators. This approach has the advantage of universality but the limitation of abstraction. In practice, legal enforcement depends on identifying specific perpetrators. The paper does not resolve this tension but acknowledges it as an area for further legal development.

14. CONCLUSION

European law already recognizes psychological violence through domestic violence legislation, workplace protections, anti-harassment frameworks, consumer protection law, data protection regulation, platform governance and artificial intelligence regulation.

GREVIO has explicitly extended the Istanbul Convention to cover the digital dimension of psychological violence through its General Recommendation No. 1 (2021). The Council of the EU has recognized cognitive warfare as an emerging hybrid threat requiring societal resilience. National legislation such as Slovenia's ZMed-1 (2025) demonstrates increasing attention to information pollution and AI transparency.

Taken together, these developments reveal a broader trend.

The historical evolution of law demonstrates a gradual expansion of protected human interests:

from life and bodily integrity,

to dignity,

to privacy and informational self-determination,

and increasingly toward **cognitive integrity**.

The rapid growth of digital influence systems, behavioural technologies, algorithmic recommendation systems, artificial intelligence, and foreign cognitive warfare capabilities suggests that cognitive integrity may become one of the next frontiers of legal protection in democratic societies.

At the same time, important regulatory gaps remain.

Political manipulation, commercial behavioural engineering, algorithmic influence systems, foreign disinformation campaigns, and cognitive dependency continue to operate largely outside traditional legal categories.



Current legal frameworks successfully address many forms of direct psychological violence but remain less capable of addressing long-term, systemic and technologically mediated forms of influence – particularly when those influences originate from foreign actors operating outside EU jurisdiction.

The emergence of cognitive dependency as a potential regulatory blind spot highlights the need for further interdisciplinary research and legal reflection.

Future legal development may therefore involve a gradual shift from protecting individuals solely against physical and psychological violence toward protecting the conditions necessary for autonomous judgment itself – regardless of whether the threat originates from domestic commercial platforms, foreign state actors, or domestic institutions.

This does not require restricting freedom of expression, political competition or democratic debate.

Rather, it requires strengthening transparency, accountability and safeguards against practices that systematically undermine cognitive autonomy – applied consistently across actor types.

The mechanisms through which psychological violence and cognitive dependency operate are analyzed in detail elsewhere (Hladnik, 2025). This paper has focused on the legal framework: how European law recognizes psychological violence, where regulatory gaps exist, and how future legal development might protect cognitive integrity.

Psychological violence should therefore be understood not only as an interpersonal phenomenon but also as a broader societal challenge connecting domestic abuse, workplace harassment, commercial manipulation, political influence, digital information environments, and foreign cognitive warfare.

The relationship among the core concepts may be summarized as follows:

Psychological Violence

(systematic impairment of autonomous judgment)



Cognitive Dependency

(chronic condition of eroded judgment)



Erosion of Cognitive Integrity

(loss of individual capacity for autonomous thought)



Threats to Democratic Resilience

(weakened public discourse, polarization, loss of trust)



↓

Challenges to State Sovereignty

(vulnerability to foreign influence, reduced capacity for autonomous governance)

↓

Challenges to Cognitive Sovereignty

(the continuous effort to preserve judgment despite competing influences)

The objective of democratic societies is not the elimination of influence.

Influence is an inevitable part of human existence – and a legitimate tool of democratic governance, commercial activity, and international relations.

The objective is the preservation of the conditions that allow individuals and societies to exercise independent judgment despite continuous exposure to competing influences, narratives and interests – and despite the fact that those influences may originate from multiple directions simultaneously (domestic commercial platforms, foreign state actors, domestic institutions, interpersonal relationships).

The art of life lies in maintaining equilibrium between doubt and determination.

A democratic society should strive to ensure that this equilibrium remains possible – for individuals, for democracy, and for the state.

FINAL THESIS

European law is gradually moving from the protection of physical integrity toward the protection of cognitive integrity.

The recognition of psychological violence, coercive control, systemic digital risks, manipulative AI systems, behavioural influence technologies, the digital dimension of psychological violence (GREVIO, 2021), and cognitive warfare (Council of the EU, 2024) suggests that cognitive autonomy may become one of the next frontiers of democratic legal development.

Whether future legal systems ultimately recognize cognitive integrity as a distinct protected legal interest remains uncertain.

What is already clear, however, is that the preservation of autonomous judgment is becoming increasingly important for the protection of human dignity, democratic resilience and the long-term pursuit of cognitive sovereignty – regardless of whether the threats to that judgment originate from domestic commercial platforms, foreign state actors, or domestic institutions.

The protection of the individual remains the foundation. Without the individual, there is no legal interest and no protection. The protection of democracy and the state follows from the protection of individuals capable of independent judgment.



A detailed taxonomy of specific mechanisms inducing cognitive dependency – including information overload, narrative repetition, emotional polarization, algorithmic echo chambers, attentional capture, and behavioural targeting – is provided in the author's accompanying work *Good Morning, Europa: A Suicide Note – and a Survival Guide* (Hladnik, 2025). That work analyzes specific techniques employed by various actors across political, commercial, and digital domains. This paper has focused on the legal framework and regulatory responses.

REFERENCES

Academic Literature

Arendt, H. (1951) *The Origins of Totalitarianism*. New York: Schocken Books.

Brcic, M. (2025) 'The Memory Wars: AI Memory, Network Effects, and the Geopolitics of Cognitive Sovereignty', *arXiv preprint*, arXiv:2508.05867. Available at: <https://arxiv.org/abs/2508.05867>.

Bublitz, J.C. (2012) 'Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination', in *Neuroscience and the Law*. Springer, pp. 1–20. Available at: <https://openscience.hamburg/de/suchen-entdecken/suchergebnis/id/df729817c10c9d8def8437345d115e8b/>.

Chomsky, N. and Herman, E.S. (1988) *Manufacturing Consent: The Political Economy of the Mass Media*. New York: Pantheon Books.

Cialdini, R.B. (1984) *Influence: The Psychology of Persuasion*. New York: Harper Business.

Clark, A. and Chalmers, D. (1998) 'The Extended Mind', *Analysis*, 58(1), pp. 7–19.

Desmet, M. (2021) *De psychologie van totalitarisme*. Antwerpen: Houtekiet. (English translation: *The Psychology of Totalitarianism*, 2022).

Farahany, N. (2023) *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology*. New York: St. Martin's Press.

Foucault, M. (1975) *Surveiller et punir: Naissance de la prison*. Paris: Gallimard. (English translation: *Discipline and Punish*, 1977).

Hladnik, G. (2025) *Good Morning, Europa: A Suicide Note – and a Survival Guide*. Libertas Europa. Available at: <https://www.amazon.de/dp/B0FY36SF6F>.

Kahneman, D. (2011) *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Klein, C.R. (2025) 'The hollowed mind: Cognitive sovereignty in the age of generative AI', *Frontiers in Artificial Intelligence*, 8, Article 1719019. Available at: <https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1719019/>.



Lanier, J. (2018) *Ten Arguments for Deleting Your Social Media Accounts Right Now*. New York: Henry Holt and Company.

Risko, E.F. and Gilbert, S.J. (2016) 'Cognitive offloading', *Trends in Cognitive Sciences*, 20(9), pp. 676–688.

Stavropoulos, N. (1996) 'Mind-Dependence and Cognitivism', in *Objectivity in Law*. Oxford: Oxford University Press, pp. 83–124.

Sunstein, C.R. (ed.) (2000) *Behavioural Law and Economics*. Cambridge: Cambridge University Press.

Sunstein, C.R. and Thaler, R.H. (2008) *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New Haven: Yale University Press.

Tögel, J. (2023) *Kognitive Kriegsführung. Neueste Manipulationstechniken als Waffengattung der NATO*. Frankfurt: Westend Verlag.

Tögel, J. (2023) 'Soft Power. Errungenschaft oder Gefahr für die Demokratie?', in Hutmacher, F. and Mayrhofer, R. (eds.) *Errungenschaften. Historische und psychologische Perspektiven auf eminente Leistungen*. Lengerich: Pabst Science Publishers.

Tögel, J. (2024) 'Kriegspropaganda damals und heute. Von den Techniken der Creel-Commission im Ersten Weltkrieg bis zum Cognitive Warfare der NATO seit 2020', in Broecker, J. and Kaltwasser, S. (eds.) *Mediensystem und öffentliche Sphäre in der Krise*. Frankfurt: Westend academics.

Tripathi, G. and Saxena, L. (2025) 'The Managed Mind: Cognitive Sovereignty as a Necessary Evolution of the Social Contract', *SRCC Journal*. Available at: <https://srcc.edu/managed-mind>.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Primary Legal Sources – European Union

European Parliament and Council of the European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union L 119, 4 May 2016.

European Parliament and Council of the European Union (2022) *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*. Official Journal of the European Union L 277, 27 October 2022.



European Parliament and Council of the European Union (2024) *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union L, 12 July 2024.

European Parliament and Council of the European Union (2024) *Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act)*. Official Journal of the European Union L, 17 April 2024.

European Parliament and Council of the European Union (2024) *Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence*. Official Journal of the European Union L, 24 May 2024.

European Parliament and Council of the European Union (2011) *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography*. Official Journal of the European Union L 335, 17 December 2011.

Primary Legal Sources – Council of Europe

Council of Europe (2011) *Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)*. Council of Europe Treaty Series No. 210. Istanbul.

GREVIO (Group of Experts on Action against Violence against Women and Domestic Violence) (2021) *General Recommendation No. 1 on the digital dimension of violence against women*. Adopted 20 October 2021. Available at: <https://www.institut-fuer-menschenrechte.de/menschenrechtsschutz/datenbanken/rechtsprechungsdatenbank-ius-gender-gewalt/detail/grevio-allgemeine-empfehlung-nr-1-2021> .

Primary Legal Sources – European Court of Human Rights

European Court of Human Rights (2008) *S. and Marper v. the United Kingdom* [GC], Applications Nos. 30562/04 and 30566/04, Judgment of 4 December 2008.

Primary Legal Sources – Slovenia

Zakon o medijih (ZMed-1) (2025) Uradni list Republike Slovenije, št. 69/2025 z dne 12. septembra 2025. Available at: https://www.uradni-list.si/_pdf/2025/Ur/u2025069.pdf .

Kazenski zakonik (KZ-1) (2008) Uradni list Republike Slovenije, št. 55/2008 z dne 6. junija 2008 (with subsequent amendments).

Secondary Sources – Institutional and Policy Documents



AKOS (Agency for Communication Networks and Services of the Republic of Slovenia) (2026) *AKOS supports the European Commission's investigation of the X platform regarding the AI tool Grok*, Press release, February 2026.

AKOS (2026) *AKOS invites evidence on risks to minors on Roblox platform*, Press release, February 2026.

Council of the European Union (2024) *Guidelines on Cognitive Warfare*. Working Party on Hybrid Threats, 4 October 2024. (Document not yet publicly released; cited from internal sources).

European Commission (2022) *Code of Practice on Disinformation*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation> .

European Institute for Gender Equality (EIGE) (2022) *Country profiles on violence against women*. Available at: <https://eige.europa.eu/gender-based-violence/country-profiles> .

European Parliament (2020) *Study: Combating psychological violence against women*. European Parliament, Directorate-General for Internal Policies, Policy Department for Citizens' Rights and Constitutional Affairs. Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/651951/IPOL_STU\(2020\)651951_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/651951/IPOL_STU(2020)651951_EN.pdf) .

European Parliament (2025) *Question for written answer E-000366/2025 to the Commission: Implementation of Directive (EU) 2024/1385 on combating violence against women and domestic violence in Greece*. Rule 138. Available at: https://www.europarl.europa.eu/doceo/document/E-9-2025-000366_EN.html .

Document: Libertas Europa

Date of completion: June 2026.