



The **C**overage and **R**eception of
the Russian-Ukrainian **C**onflict

Legal Context

Media, Democracy and Disinformation

Author: Rafał Krzysztof Matusiak

University of Opole

Lucian Blaga University of Sibiu

Binding EU legislation

- **Digital Services Act (DSA)** — Regulation (EU) 2022/2065: risk-assessment/mitigation duties for very large platforms incl. systemic risks like disinformation; transparency and crisis-response tools.
- **European Media Freedom Act (EMFA)** — Regulation (EU) 2024/1083: safeguards for media pluralism/independence (relevant to state influence, editorial interference and the information environment).
- **Audiovisual Media Services Directive (AVMSD)** — Dir. (EU) 2018/1808: rules for video-sharing platforms; encourages co/self-regulation against harmful content incl. disinformation.
- **Transparency & Targeting of Political Advertising** — Regulation (EU) 2024/900: disclosure/targeting limits to curb manipulation and foreign interference around elections.
- **EU restrictive measures addressing propaganda/disinformation in the Russia context** — Council acts amending the sanctions regime and related jurisprudence.

The European Media Freedom Act



(Regulation (EU) 2024/1083)

Here are provisions that address disinformation, information manipulation, and foreign information interference:

Recital (4) explicitly states that

“global online platforms act as gateways to media content, with business models that tend to disintermediate access to media services and amplify polarising content and *disinformation*.”

Recital (6) further adds that

“regulatory cooperation between national authorities is key to ensuring that media market players ... that systematically engage in *disinformation or information manipulation and interference* do not benefit from the scale of the internal market.”

Article 26–27 (Monitoring Exercise and Evaluation) require the European Commission to continuously monitor:

“risks of *foreign information manipulation and interference*”

and to provide regular reports including “a detailed analysis of media markets ... and risks of *foreign information manipulation and interference*.”

Article 19(1)(c) on structured dialogue between media and large platforms mentions that such dialogue should

“monitor adherence to self-regulatory initiatives which aim to protect users from harmful content, including *disinformation* and ***foreign information manipulation and interference***.” (Examples of FIMI → slide 14)

UNREADABILITY OF LEGALESE

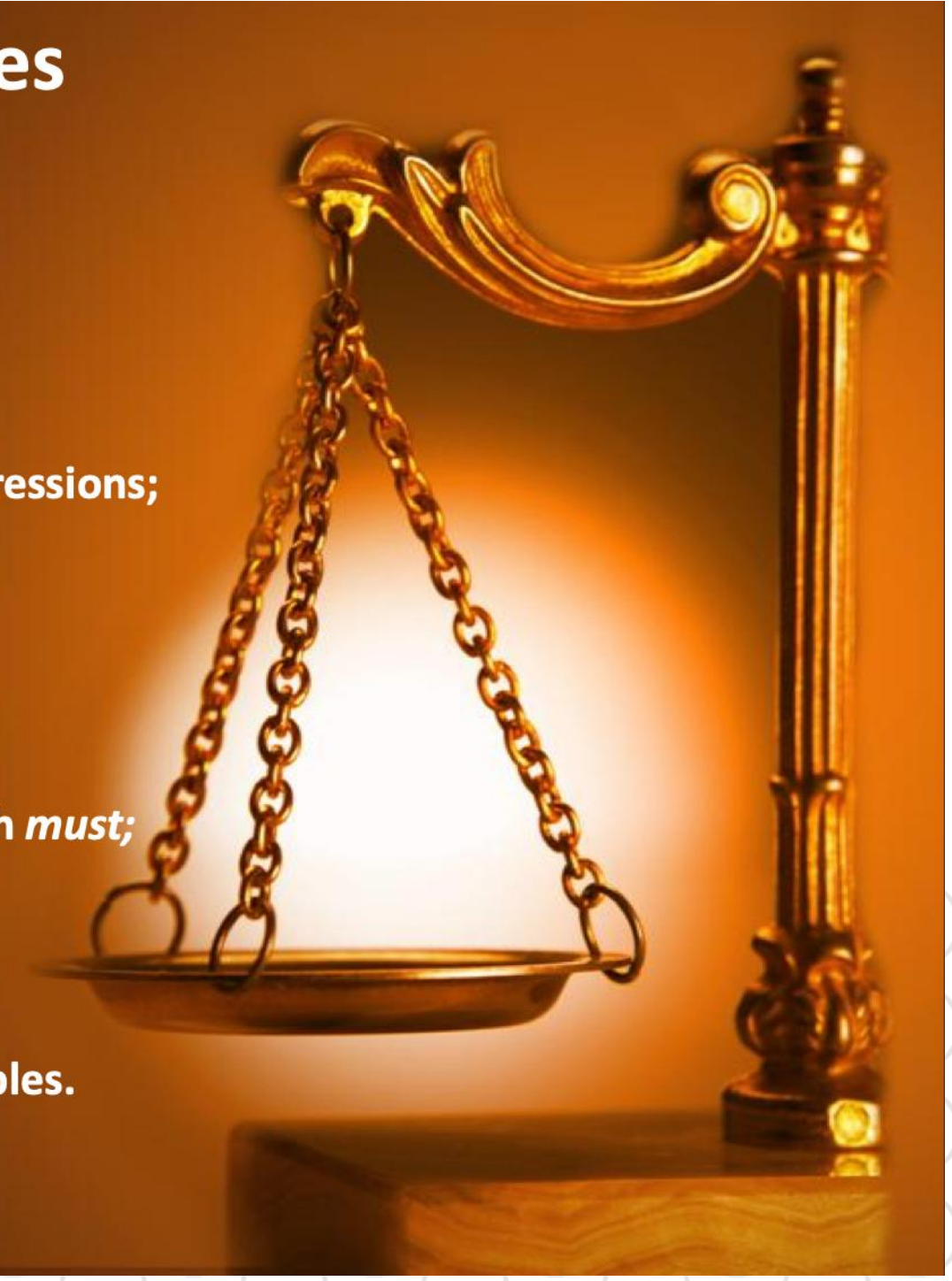
‘the language of law must not be foreign to the ears of those who are to obey it’.

A peculiar cant or jargon of their own, that no other mortal can understand, and wherein all their laws are written.
(Jonathan Swift, Gulliver’s travells)

He read it [the will] with a certain relish, lingering over its more obscure phraseology, and savouring its legal technicalities.
(Agatha Christie, Hercule Poirot’s Christmas)

Some of members of the High Court of Chancery bar ought to be [...] mistily engaged in one of the ten thousand stages of an endless cause, tripping one another up on slippery precedents, groping knee-deep in Technicalities, running their goat-hair and horsehair warded heads against walls of words and making a pretence of equity with serious faces, as players might.
(Charles Dickens, Bleak House)

Plain English Principles

- 
- I. Favour informal language;
 - II. Don’t write too long sentences;
 - III. Avoid redundancy;
 - IV. Don’t use archaisms and Latin expressions;
 - V. Reduce the use of the passive;
 - VI. Limit nominalization;
 - VII. Employ personal pronouns;
 - VIII. Replace the modal verb *shall* with *must*;
 - IX. Use verbs in the present simple in the indicative mood if possible;
 - X. Use finite verbs rather than participles.

GUNNING FOG INDEX FORMULA

Gunning Fog Index = $0.4 \times [(\text{total sentences} / \text{total words}) + 100 \times (\text{total words} / \text{complex words})]$

Where:

- **Total words** = number of words in the text.
- **Total sentences** = number of sentences in the text.
- **Complex words** = words with **three or more syllables**, excluding:
 - proper nouns (names),
 - familiar jargon or compound words,
 - verbs made longer by adding suffixes like *-es*, *-ed*, or *-ing*.

Shifts in sentence length

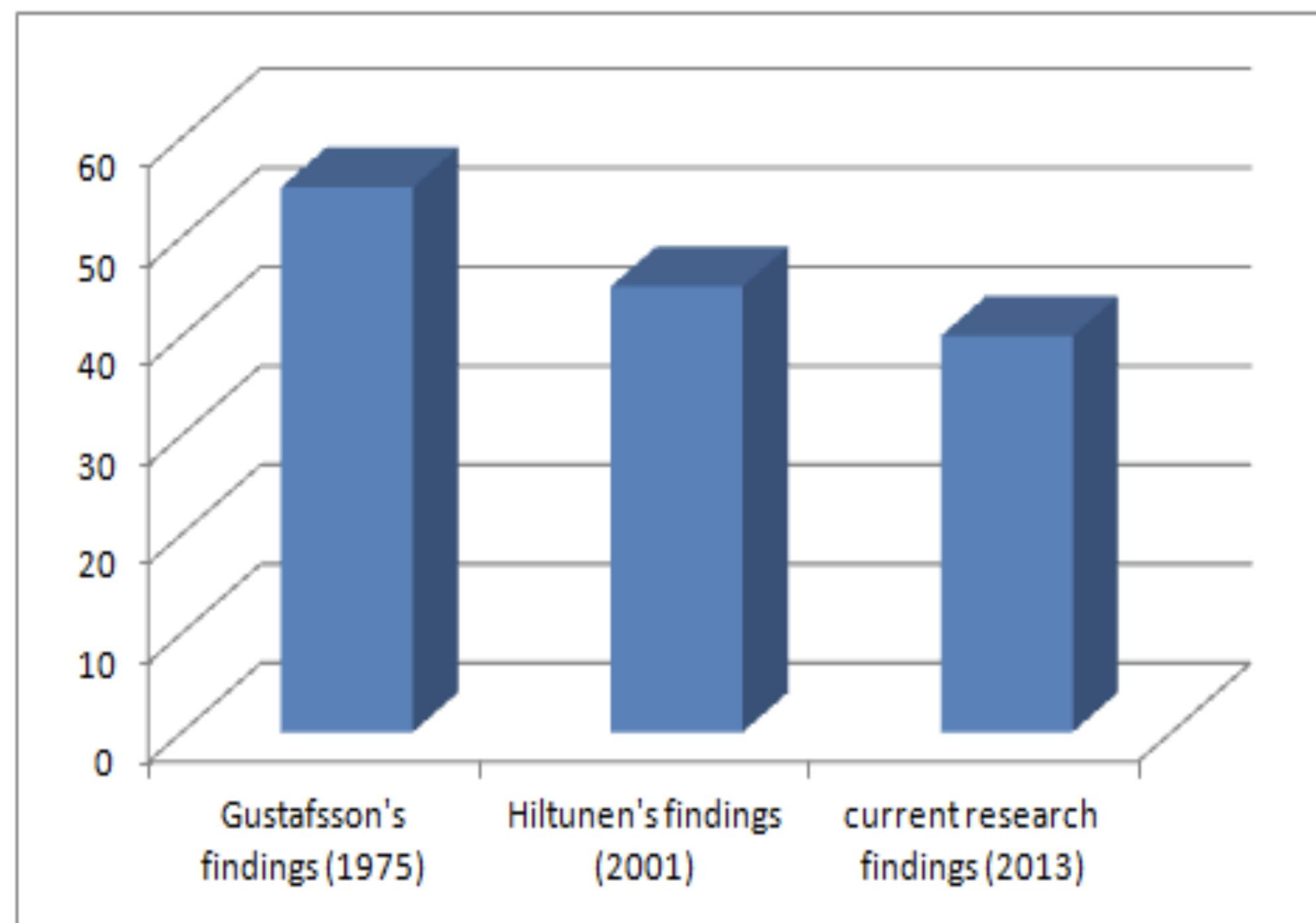


Figure 1. The comparison of the findings on sentence length achieved by Gustafsson (1975), Hiltunen (2001), and the current research findings (2013).

UNREADABILITY OF Digital Services Act (DSA)

That corresponds to **postgraduate level readability** — understandable mainly to **lawyers, policymakers, or domain experts**.

For your short summary phrase

“risk-assessment/mitigation duties for very large platforms incl. systemic risks like disinformation; transparency and crisis-response tools”

That’s a single dense nominal phrase, not a full passage, but if treated as a sentence:

- ~13 words
- 5 complex words (“assessment,” “mitigation,” “systemic,” “disinformation,” “transparency”)
- Complex-word ratio $\approx 38\%$

$$0.4 \times (13 + 100 \times 0.38) = 0.4 \times (13 + 38) = 0.4 \times 51 = 20.4$$

Estimated Gunning Fog Index: ~20 — still **very difficult**, roughly **academic/technical** level.

UNREADABILITY OF Digital Services Act (DSA)

Article 34(1) of the DSA:

“Providers of very large online platforms and of very large online search engines shall identify, analyse and assess any significant systemic risks stemming from the functioning and use made of their services in the Union, including the dissemination of illegal content through their services, any actual or foreseeable negative effects for the exercise of fundamental rights, and any intentional manipulation of their service with an actual or foreseeable negative effect on civic discourse, electoral processes and public security.”

Word count: 79 words

Sentence count: 1

Complex words (≥ 3 syllables) ≈ 35 ($\approx 44\%$)

Calculation

$$0.4 \times (79 + 100 \times 0.44) = 0.4 \times (79 + 44) = 0.4 \times 123 = 49.2$$

Estimated Gunning Fog Index: ≈ 49

UNREADABILITY OF Digital Services Act (DSA)

The DSA is a dense legal document written in formal EU legal English — long sentences, extensive sub-clauses, and legal jargon.

- Average sentence length: **40 words/sentence**
- Complex-word ratio: **27.5 %**
- Plugging those into the formula: $0.4 \times (40 + 100 \times 0.28) = 0.4 \times (40 + 28) = 0.4 \times 68 = 27.2$

Estimated Gunning Fog Index: ~26–28

The Transparency Paradox of the DSA



The Paradox

- The **Digital Services Act** aims to make online communication transparent, fair, and accountable.
- Yet the **Act itself is nearly unreadable** — written at a **postgraduate (Gunning Fog 26–28)** level.
- A regulation about **clarity and accessibility** fails its own readability test.

Why It's a Problem

- Complex legal language **limits accessibility** for citizens, SMEs, and civil society groups.
- The people expected to **comply with or benefit from** the Act often **can't easily understand** its provisions.
- **Transparency in content moderation** begins with transparency in the law itself.

TASK 1: Read one article and select the description (A–H) that best matches its content.

Provision	Key content relevant to disinformation / amplification / misleading content
Article 14	(A) Mandates concrete mitigation and cooperation measures.
Article 26	(B) Increases transparency of advertising and targeting systems.
Article 33	(C) Requires systematic assessment of disinformation-related risks.
Article 34	(D) Defines which platforms are subject to stricter scrutiny.
Article 35	(E) Promote cooperative mechanisms (codes and crisis protocols) for managing disinformation and manipulation risks.
Article 38	(F) Establishes public ad repositories to track political/issue ads.
Article 39	(G) Ensures transparency and adjustment of recommender systems to reduce harmful amplification.
Article 44 & 48	(H) Ensures transparent, fair, and rights-respecting moderation policies.





Provision	Key content relevant to disinformation / amplification / misleading content
Article 14	Ensures transparent, fair, and rights-respecting moderation policies. (H)
Article 26	Increases transparency of advertising and targeting systems. (B)
Article 33	Defines which platforms are subject to stricter scrutiny. (D)
Article 34	Requires systematic assessment of disinformation-related risks. (C)
Article 35	Mandates concrete mitigation and cooperation measures. (A)
Article 38	Ensures transparency and adjustment of recommender systems to reduce harmful amplification. (G)
Article 39	Establishes public ad repositories to track political/issue ads. (E)
Article 44 & 48	Promote cooperative mechanisms (codes and crisis protocols) for managing disinformation and manipulation risks. (F)

Provisions relevant to disinformation / amplification / misleading content (DSA)



Provision	Key content relevant to disinformation / amplification / misleading content
Article 33 (Designation of very large services)	Triggers the special regime (Articles 34–40) for platforms with “systemic reach,” where disinformation risk is most acute.
Article 34(Risk assessment)	Obligates VLOPs / VLOSEs to identify, analyse and assess systemic risks, including dissemination of illegal content and negative effects on the exercise of fundamental rights (including freedom of expression, pluralism of the media) and negative effects on civic discourse and electoral processes. Sub-paragraph (2) requires consideration of intentional manipulation, amplification, inauthentic use, algorithmic systems, advertising systems in assessing those risks.
Article 35 (Risk mitigation)	Once risks are identified, VLOPs / VLOSEs must adopt proportionate mitigation measures, which may include: • adapting content moderation speed/quality (especially for types of illegal content). • testing and adapting algorithmic systems / recommender systems. • adapting advertising systems, and limiting presentation of ads that may exacerbate risk. • enhancing internal processes, resources, supervision for risk detection. • cooperating with trusted flaggers and other platforms, or via codes of conduct / crisis protocols.
Article 38(Recommender systems)	Requires transparency about how recommender systems work, and also that risk mitigation includes adjustments or constraints to such systems where needed (e.g. reducing amplification of harmful content).

Provisions relevant to disinformation / amplification / misleading content



Provision	Key content relevant to disinformation / amplification / misleading content
Article 26 (Advertising on online platforms)	All platforms must present ads to users in a clear, identifiable way. VLOPs / VLOSEs must provide more detailed transparency about who sponsors ads, targeting parameters and major influencing factors. This helps expose manipulative or misleading ad campaigns.
Article 39 (Ad repositories)	VLOPs/VLOSEs must maintain a searchable repository of political / issue ads (with their performance metrics). This transparency helps researchers & regulators detect disinformation / manipulation campaigns.
Article 45 & 48 (Codes of conduct, crisis protocols)	Encourages voluntary or co-regulatory measures or protocols (e.g. codes of practice) aimed at developing best practices including for election integrity, misinformation, and crisis scenarios.
Article 14 (Terms and conditions)	Requires platforms to disclose their content moderation policies, algorithmic decision-making, and procedures. Platforms must apply those restrictions in a diligent, objective, proportionate way, taking into account freedom of expression, pluralism of media.

SUMMARY OF THE DSA PERSPECTIVE

Category	Legal Status	Regulatory Focus	Platform Responsibility
Illegal Content	Prohibited by law	Removal, cooperation with authorities	Immediate removal after notice
Disinformation	Not illegal but harmful	Transparency & risk mitigation	Reporting, code of conduct adherence
Manipulation	Behavioural/systemic issue	Algorithmic accountability, audit	Mitigation of amplification & distortion

KEY ELEMENTS IN THE FIMI DEFINITION

Element	Description
Pattern of behaviour	It is not a one-off; rather repeated or systematic activity.
Threat or negative impact	Aimed (or with potential) to harm democratic values, institutions, political processes.
Manipulative character	Involves covert or deceptive techniques, not merely opinion or propaganda.
Intentional & coordinated	Deliberate orchestration (not random), possibly across actors and platforms.
Actors	Can be state actors, non-state actors, or proxies (inside or outside their own territory).
Often non-illegal	Many of these acts may not violate criminal law directly, but still pose risks.
Hybrid context	Part of a broader set of tools (information + cyber + influence) used in modern conflict / power competition.

Case studies:

- *Doppelgänger,*
- *Storm-1516,*
- *Moldova AI ops,*
- *NewsFront,*
- *Meta covert campaigns,*
- *Italian Twitter bots,*
- *MH17 troll campaigns*

TASK 2: Each group should:

- 1. Summarise the operation** in 5 bullet points:
Who, Where, How, Goal, Outcome.
- 2. Identify which manipulative techniques**
appear (e.g. fake domain, deepfake,
emotional language, false translation, social-
bot amplification).
- 3. Map target audience and intended
emotional effect** (e.g. fear, anger, distrust).

Case studies:

- *Doppelgänger,*
- *Storm-1516,*
- *Moldova AI ops,*
- *NewsFront,*
- *Meta covert campaigns,*
- *Italian Twitter bots,*
- *MH17 troll campaigns*

TASK 3: After group work (10–15 minutes), discuss:

- What was hard to classify and why?
- Can disinformation ever become illegal content? (e.g., public incitement to hatred)
- What are the ethical limits of content moderation vs. freedom of speech?

CASE STUDY

Case	Description	Type
1. “We know where you live” tweet targeting a candidate	A user posts personal address and threats of violence against an MEP candidate.	
2. Viral TikTok clip	Claims that “EU elections are cancelled because of a secret treaty with China.”	
3. Bot-driven campaign	Hundreds of identical Twitter accounts post “Vote for X — everyone else is corrupt!” within 3 minutes.	
4. Meme saying “Vaccines kill 1 in 10 children.”	False health data, but not tied to a specific crime.	
5. YouTube comment advertising counterfeit EU passports.	Explicit illegal offer.	
6. Platform algorithm pushing polarizing political content.	Amplifies division, even if posts are not illegal.	
7. Satirical fake news website clearly marked as parody.	Intent is humorous, not deceitful.	

CASE STUDY



Case	Description	Type
1. “We know where you live” tweet targeting a candidate	A user posts personal address and threats of violence against an MEP candidate.	Illegal Content → Report and remove immediately, notify authorities.
2. Viral TikTok clip	Claims that “EU elections are cancelled because of a secret treaty with China.”	Disinformation. → Fact-check and publish a correction; the platform should flag it as misleading.
3. Bot-driven campaign	Hundreds of identical Twitter accounts post “Vote for X — everyone else is corrupt!” within 3 minutes.	Manipulation. → Investigate inauthentic behaviour; transparency report required under DSA.
4. Meme saying “Vaccines kill 1 in 10 children.”	False health data, but not tied to a specific crime.	Disinformation.
5. YouTube comment advertising counterfeit EU passports.	Explicit illegal offer.	Illegal Content.
6. Platform algorithm pushing polarizing political content.	Amplifies division, even if posts are not illegal.	Manipulation.
7. Satirical fake news website clearly marked as parody.	Intent is humorous, not deceitful.	Neither illegal nor harmful → protected under freedom of expression.

Spot the Difference — Disinformation, Manipulation, or Illegal Content?

TASK 4:

- Distinguish between illegal content, disinformation, and manipulation according to the DSA framework.
- Justify your classification decisions using legal and ethical reasoning.
- Reflect on the responsibilities of journalists and platforms in handling such content.

Tracing Liability and Responsibility

Form groups of 3–4. Each group is assigned one of the following cases from the *DSA*.

TASK 5:

- Summarize your case in one paragraph (facts + decision).
- Identify which values or rights are in tension (e.g., privacy vs. expression, transparency vs. innovation).
- Prepare a 3-minute briefing to present your findings to the class.

Tracing Liability and Responsibility

Group	Case	Focus Area
1	<i>Delfi AS v. Estonia</i>	Platform liability for user comments
2	<i>MTE & Index.hu Zrt v. Hungary</i>	Contextual limits to intermediary liability
3	<i>GS Media BV v. Sanoma Media</i>	Hyperlinking and facilitation of illegal content
4	<i>Google Spain v. AEPD</i>	Right to be forgotten and visibility control
5	<i>TikTok Privacy Case (Ireland DPC)</i>	Manipulative design and consent
6	<i>Netherlands v. SyRI</i>	Algorithmic transparency and surveillance
7	<i>Dark Patterns Case (Germany)</i>	Consumer manipulation and fairness

EXTRA TASK: Simulation: Digital Democracy Hearing

The class acts as a **European Parliamentary Committee** debating the question:

“Should online platforms be legally required to actively detect and label disinformation?”

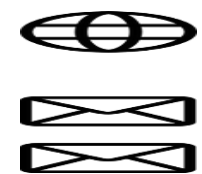
Roles:

- Platform Representatives (Meta, TikTok, X)
- Civil Society Advocates
- Data Protection Authorities
- Journalists and Fact-Checkers
- Members of the European Parliament

Each role should:

- Cite at least **one case** from the packet to justify their stance.
- Refer to **relevant DSA provisions** (e.g., risk assessment, transparency reporting, systemic risks to democracy).
- Propose **one amendment** to the DSA to improve democratic resilience against disinformation.

Contact

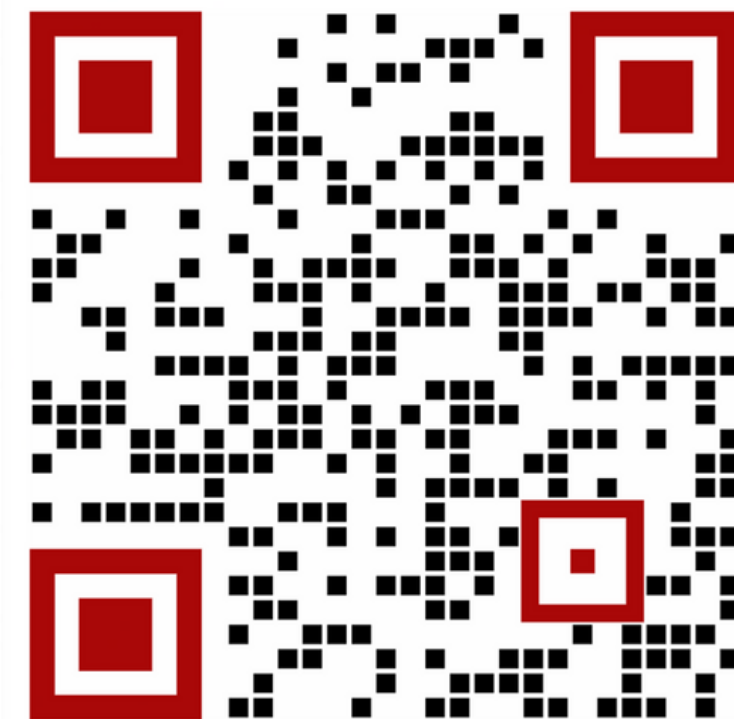


rafalkrzysztof.matusiak@ulbsibiu.ro

Find us on our social media!



CORECON
website



grants.ulbsibiu.ro/corecon



**Funded by
the European Union**



forthem.

Fostering Outreach
within European Regions,
Transnational Higher Education
and Mobility



CORECON

The **C**overage and **R**eception of
the Russian-Ukrainian **C**onflict

Funding attribution

The project was funded by the EU's NextGenerationEU instrument through the National Recovery and Resilience Plan of Romania – Pillar III-C9-I8, second round, managed by the Ministry of Research, Innovation and Digitalization, within the project entitled The Coverage and Reception of the Russian–Ukrainian Conflict in Polish, Romanian and English-Language Media: A Comparative Critical Discourse Study with Recommendations for Journalism Training (CORECON), contract no. 760244/28.12.2023, code CF 25/27.07.2023.

