A True Digital Democracy Cannot Be Copied by Autocracies! (August 2026)

"Trusted WEB 4.0 is the Integration of all resources available via the Web into an overall system.

Machines, devices and people are globally accessible, organized in decentralized, anonymous structures.

Trusted WEB 4.0 maps pre-digital social structures.

The value chains are being reorganised.“
(Olaf Berberich, 2007)

A Genuine Digital Democracy Cannot Be Copied by Autocracies!

Research Report on the Threat to Democratic Systems by Digital Manipulation, Remote-Controlled Gang-Like Appearance, and Judicial Helplessness

---

📌 Executive Summary

The Core Thesis

A genuine digital democracy does not currently exist. The current digital reality enables autocratic actors, organized networks, and **remote-controlled gang-like structures** to systematically undermine democratic processes – **without the rule of law being able to effectively counter them.**

This study is based on **concrete, court-known facts** from an **11-year criminal proceeding** (case reference anonymized) and current **homeowners' association (WEG) proceedings** (case reference anonymized), which document a **pattern of remote-controlled gang-like appearance**. Further evidence can be found at www.finders.de/?s= followed by the respective year.

The Five Core Problems

Problem	Mechanism	Consequence	Evidence
Hybrid Warfare	Individual "disposable agents" with clearly identifiable aggressor (e.g., Russia)	Justice can only act with identifiable perpetrators and evidence – pinprick tactics remain unpunished	Internationally documented
Remote-Controlled Gang-Like Appearance	**Remotely controlled actors** pursuing a common goal **without being aware of the criminal nature of their actions**	No lawyer can be found for victims; legal aid fails	**Criminal Proceedings (GraTeach, see Finders Archive)**
Systemic Remote Control	Technical infrastructure enables control of entire regions (Example: GraTeach case)	Democracy is "remotely controlled" – evidence exists, but justice cannot intervene	**GraTeach Case**

Problem	Mechanism	Consequence	Evidence
Lawyer Crisis	Systematic manipulation/elimination of all legal representatives	Affected individuals **can no longer effectively defend themselves**	Remote-Controlled Gang-Like Appearance
Judicial System Blindness	Courts **do not recognize patterns** or ignore them	**Structural denial of justice**	**WEG Proceedings** (Remote-Controlled Gang-Like Appearance)

The Legal Dilemma

- **Article 20(4) of the Basic Law (Right to Resistance)** is **not practical for individuals** when they must defend themselves **without a lawyer** and **only in writing** against systemic attacks.
- The **EU** delegates cases like GraTeach to national justice systems – which, however, **fail due to structural limitations**.
- **"All state authority derives from the people" (Article 20(2) GG)** is undermined when those who commit to the constitutional order are **disabled through digital data and remote-controlled gang-like appearance**.
- **§ 128 ZPO (written proceedings)** and **mandatory legal representation** are **misused as tools of exclusion**.

The Solution: Trusted WEB 4.0 with GISAD and EU-D-S

Trusted WEB 4.0 – Definition by Olaf Berberich (2007):

"Trusted WEB 4.0 is the integration of all resources available via the web into a comprehensive system. Machines, devices, and people are globally accessible, organized in decentralized, anonymized structures. Trusted WEB 4.0 maps pre-digital societal structures. The value chains are newly organized."

Olaf Berberich has filed several patents, for example for the finder search engine and WAN anonymity. The solution consists of three components:

1. **GISAD** (Global Institute for Structure Relevance, Anonymity, and Decentralization) – **to be established as a result of the identified problems to create expert opinions and guidelines**. More information at www.gisad.eu.
2. **EU-D-S** (European Digital System) – the **technical infrastructure**, provided by www.get-primus.com, in which all participants are registered with WAN anonymity.
3. The **EU-D-S Constitution** governs the collaboration and value creation of participants in the EU-D-S at https://finders.de/wp-content/uploads/2026/06/EU-D-S-Verfassung-en-US.pdf.

Functionality:

- **Closed System**: All participants are **registered with WAN anonymity**.
- **Project Review**: **All projects** are reviewed by GISAD for **societal structural relevance** – otherwise, they **do not enter the EU-D-S**.
- **De-Anonymization**: Only possible **in individual cases by court order**.
- **Protection Mechanism**: Potentially threatened individuals can protect themselves by **communicating only within the EU-D-S**.

"Remote-controlled gang-like appearance: Whoever has sufficient information about the entire environment can disable or control anyone without them recognizing the connection. The only solution is that everyone can be de-anonymized in individual cases by court order."

Solution Paths

1. **Judicial Self-Commitment**: Protection mechanisms to prevent **public harm** caused by the obstruction of individuals.
2. **EU-Wide Obligation to Act**: When national justice fails, the EU must be able to intervene.
3. **Digital Resilience**: Technical and legal frameworks that make **remote-controlled manipulation impossible**.
4. **EU-D-S Constitution + GISAD + EU-D-S**: **System change through closed, controlled systems** – without new bureaucracy.

🎯 Introduction: Why This Study Is Necessary

The Initial Situation

Digitalization has **not strengthened democracy, as often proclaimed**, but has made it **more vulnerable**. While autocracies use digital tools specifically for suppression and manipulation, democratic states lack effective defense mechanisms. **This study proves with concrete cases that the problem is not theoretical but acute and systemic.**

The Empirical Basis

This study is based on:

1. **Letter to the President of the Court (File No. 3132-1582)** – Concrete listing of the events of the **GraTeach insolvency and WEG proceedings**.
2. **An 11-year criminal proceeding (GraTeach)** – involving **systematic lawyer manipulation**.
3. **Current WEG proceedings** (Remote-Controlled Gang-Like Appearance: 3rd Attack) – Documentation of **systematic obstruction**.
4. **Finders Archive** – Further information at www.finders.de/?s=Year (enter year).

Case Studies

1. **GraTeach**: Provable **remote control of a state administration** through digital infrastructure.
2. **A Criminal Proceeding**: **Remote-controlled gang-like appearance** in its pure form – all legal representatives manipulated or excluded.
3. **Hybrid Warfare from Russia**: Identifiable aggressors, but unpunished "disposable agents".

Research Questions

This study answers five central questions:

1. How can the state protect citizens when their obstruction **causes public harm**?
2. Why **must** the EU act when national justice fails?
3. How can **"All state authority derives from the people"** be preserved in an era of digital total surveillance?
4. How does **remote-controlled gang-like appearance** work concretely – and why is it **not the same as decentralized networks**?
5. How can **Trusted WEB 4.0 with GISAD and EU-D-S** solve the problem **technically and legally**?

🔍 Part 1: Judicial Helplessness and Its Consequences – Concrete Evidence

---

1.0 Definition: What Is Remote-Controlled Gang-Like Appearance?

Remote-Controlled Gang-Like Appearance (according to the author's experience):

"Many people are controlled remotely for a goal they do not know. The result is the same as with gang-like structures, but criminally, individuals cannot be prosecuted because they are not aware of the punishable act."

Distinction from Decentralized Networks:

Criterion	Remote-Controlled Gang-Like Appearance	Decentralized Networks
Control	Remotely controlled actors with **central intelligence** that knows the goal	**Autonomous actors** without central control
Actors' Awareness	Act **unwittingly** as part of a system	Act **autonomously**
Judicial Grasability	**Hard to grasp** (no direct perpetrator evidence)	**Hard to grasp** (no central instance)
Difference	There is **a perpetrator group with knowledge** – it is just **not directly provable**	**No central intelligence**

1.1 The Difference: Hybrid Warfare vs. Remote-Controlled Gang-Like Appearance

Hybrid Warfare (Example: Russia)

- **Aggressor Identifiable**: Yes (state actor)
- **Perpetrator Structure**: Individual "disposable agents" with limited lifespan
- **Judicial Reaction**: **Possible**, if evidence is available
- **Problem**: Pinprick tactics – many small attacks, each below the threshold of criminal liability

Remote-Controlled Gang-Like Appearance (Example: Criminal Proceeding)

- **Aggressor Identifiable**: **Yes, but not usable in court** (remotely controlled networks with central intelligence)
- **Perpetrator Structure**: **Remotely controlled individuals** (lawyers, experts, judges) who **do not understand their actions as part of a system**
- **Judicial Reaction**: **Impossible** – no lawyer can be found; legal aid does not apply
- **Problem**: Systematic elimination of critics **without direct criminal consequences**

- **Evidence**: **Letter to the President of the Court (File No. 3132-1582, anonymized)** – Chronology of lawyer manipulation

Conclusion: The judiciary can only act if it has a **perpetrator** and **evidence**. With remote-controlled gang-like appearance, **both conditions are manipulated** – the perpetrators act **unwittingly**, and the evidence is **systematically suppressed**. The judiciary itself can be part of the remotely controlled system.

1.2 The GraTeach Case: Remote Control as Reality

What Happened:

- **At the beginning of the proceeding**: A **law student** filed a **false criminal complaint** with the public prosecutor's office.
- **During the course**: The **insolvency administrator** only acted **against the affected person**, did **not pay the maintenance money in the account** – even though its payment would have ended the criminal proceedings.
- A **tax advisor** and lawyer discussed **all details** with the affected person: **"If we have done something wrong, I will refer to you."**
- A **lawyer** applied for **suspension of the criminal proceedings** until the administrative court proceedings. The administrative court later found **no pre-insolvency shortcomings** – yet **the lawyer was forced to resign from the mandate**.
- A **public defender** took over the defense – **without objection from the affected person**, as they accepted it as possible help from the tax advisor.
- **In the civil proceedings**: The **agreed sum was paid**, even though the prerequisite (pre-insolvency shortcomings) was **not met** by the administrative court proceedings. The district government coerced **payment of interest** under **threat of an enforcement order**, which were not agreed upon.
- **In the appeal proceedings (1st attempt)**: The court signaled **discontinuation of the proceedings**. **4 hours before the appointment**, **a lawyer's license was revoked** – allegedly due to a conflict with a side activity. **Effect**: The court was intimidated – the proceedings continued. **No judge wanted to touch the case anymore.**
- **At the end of the proceedings**: **A defender and a lawyer** made **arrangements with the court – without the knowledge of the affected person**. The affected person was put under unexpected pressure to accept a suspended sentence.
- **Another lawyer** was **subject to disciplinary action** when they wanted to enforce copyright claims.
- **Current Status**: Even in the **Netherlands, the affected person can no longer find a lawyer** willing to take the case, despite it involving non-barred copyright claims of considerable value.

Why This Persists to This Day:

- **Psychological Effect**: "What cannot be, must not be" – the inconceivability protects the **central intelligence** behind the remote control.
- **Judicial Gap**: No court can act against **remote control** if **no natural person can be identified as the perpetrator**.
- **Systemic Blindness**: The **patterns** are not recognized or are **deliberately ignored**.

- **Evidence Problem**: **All evidence** (expert opinions, documents) is **manipulated or suppressed**.

1.3 The Lawyer Crisis: When Legal Protection Is Systematically Prevented

The Consequence:

"When the state does not protect the citizen, and the citizen cannot protect themselves, the rule of law collapses. When one lawyer after another is manipulated or excluded, only the written path remains – but this is also blocked by mandatory legal representation and the obligation for oral proceedings."

Current Status (September 2026):

- The affected person has **no legal representation anymore** – all lawyers have been **manipulated, intimidated, or excluded**.
- **Written proceedings** are the **only option** – yet courts **ignore written submissions**.
- **Mandatory legal representation** is **misused as a tool of oppression**. Self-representation before the regional court is not possible.

⚖️ Part 2: The Five Research Questions – Analysis and Solution Approaches

---

◇ Question 1: Judicial Self-Commitment vs. Protection Against Public Harm

The Current Situation:

- **No Self-Commitment**: The judiciary does not see itself as obligated to **preventively** act against structural discrimination.
- **Reactive Approach**: Action is only taken when concrete damage occurs – often too late.
- **Individual Focus**: The protection of the individual is the priority, not the protection of the **system**.
- **Systematic Ignorance**: Courts **do not recognize patterns** or **refuse to see them**.

The Problem: Systemic Disadvantage as Public Harm

When a citizen is hindered by digital manipulation and remote-controlled gang-like appearance, it triggers **ripple effects**:

Solution: Expand Judicial Protection Obligations

Proposal 1: Preventive Injunction Claims

- **Mechanism**: Citizens can **file lawsuits before** damage occurs if a **systemic threat** is provable.
- **Example**: If digital infrastructure is used for remote control (GraTeach), **immediate intervention** can be demanded.
- **Legal Basis**: Expansion of § 1004 BGB (removal and injunctive relief) to **systemic threats**.
- **Accelerated Procedure** for cases involving **remote-controlled gang-like appearance**.

Proposal 2: Collective Legal Protection

- **Mechanism**: Affected individuals can join **litigation communities**.
- **Advantages**:
  - Pooling of resources against powerful opponents.
  - Higher chances of success through combined knowledge.
  - Political signaling effect.
- **Implementation**: Expansion of the **model declaratory action** (§ 606 ZPO) to digital manipulation and remote-controlled gang-like appearance.
- **State Financing** for lawsuits against **systemic threats**.

Proposal 3: State Protection Duty for Systemic Relevance

- **Principle**: If the obstruction of a citizen **endangers the functioning of democracy**, the state **must actively intervene**.
- **Criteria**:
  - Provable systemic threat.
  - Lack of individual defense possibilities.
  - Public interest in defense.
- **Legal Basis**: Article 20(4) GG (Right to Resistance) **combined with** Article 28(1) GG (Rule of Law Principle).
- **Automatic Review** by GISAD whether a case is **societally structurally relevant**.

Conclusion for Question 1

Approach	Effectiveness	Feasibility	Cost	Novelty
Preventive Lawsuits	★★★★	★★★	Medium	Accelerated Procedure
Collective Legal Protection	★★★★★	★★★★	High	State Financing
State Protection Duty	★★★★	★★	High	GISAD Review

Recommendation: Combination of all three approaches, with a focus on **collective legal protection with state financing** as the fastest solution.

◇ Question 2: Why the EU Must Act When National Justice Fails

The Current Situation: GraTeach and WEG Proceedings as Examples

- **EU Reaction**: Referral back to national justice.
- **Problem**: National justice **cannot act** (see Part 1) – and **does not want to act** (systemic ignorance).
- **Consequence**: **Gap in legal protection** at the European level.
- **Documented Evidence** of systemic manipulation exists – but is **not appreciated**.

Why the EU Is Responsible

1. Principle of Subsidiarity (Article 5 TEU)

- **Definition**: The EU acts only when objectives can be **better achieved at Union level**.
- **Application to Digital Democracy**:
  - National justice is **overwhelmed** by cross-border digital manipulation.
  - Only the EU can set **uniform standards**.
  - Only the EU has the **resources** for effective defense.
  - Only the EU can provide **EU-D-S** as **technical infrastructure**.

2. Solidarity Clause (Article 222 TFEU)

- **Content**: The EU and the Member States act **jointly** when a Member State is affected by a **natural or man-made disaster**.
- **Application**: Digital attacks on democracy are a **"man-made disaster"**.
- **Consequence**: The EU **must** intervene if a Member State (e.g., Germany) is affected.
- **Remote-controlled gang-like appearance** is a **systemic disaster** for the rule of law.

3. Values of the Union (Article 2 TEU)

- **Rule of Law Principle**: The EU is founded on **respect for human dignity, freedom, democracy, equality, and the rule of law**.
- **Obligation**: The EU **must actively protect** these values.
- **Problem**: When national justice fails, EU values are **directly threatened**.
- **GraTeach and WEG cases** prove that the **rule of law in Germany is being systematically undermined**.

How the EU Could Act (Without New Bureaucracy!)

Measure	Description	Legal Basis	Advantage
Technical Infrastructure EU-D-S	**Technical platform** for Trusted WEB 4.0 – **without new bureaucracy**	EU Regulation	Protected by design
European Collective Legal Protection	Affected individuals can **sue directly before EU courts**	Extension of the **EU Charter of Fundamental Rights** (Article 47)	Bypassing national judicial bottlenecks
Sanctions Against Digital Attackers	**European Magnitsky Acts** for digital manipulation	EU Sanctions Regime	Deterrence through economic consequences

---

Counterarguments and Rebuttals

Counterargument	Rebuttal	New
"National Sovereignty"	Digital threats know **no borders** – national solutions are **inadequate**	✗
"Too Expensive"	The cost of **inaction** (collapse of democracy) is **infinitely higher**	✗
"Technically Not Feasible"	**EU-D-S proves the opposite** – the technology exists	☑
"New Bureaucracy"	**EU-D-S is a technical platform, not a bureaucracy**	☑

Conclusion for Question 2

The EU not only has the right but the obligation to act. The current mechanisms (referral to national justice) are **inadequate** and endanger the **very existence of the Union**.

With **EU-D-S**, the EU can act **without creating new bureaucracy**.

"If the EU fails on this issue, it fails in its most fundamental task: protecting democracy. But with EU-D-S, it now has the tool to do it right."

◇ Question 3: How Can "All State Authority Derives from the People" Be Preserved in the Digital Age?

The Problem: Digital Exclusion Through Remote-Controlled Gang-Like Appearance

- **Mechanism**: Through **data surveillance**, **digital manipulation**, and **remotely controlled actors**, critics can be **disabled**.
- **Examples from the Criminal Proceeding**:
  - **2001–2009**: **All lawyers** were **manipulated, intimidated, or excluded**.
  - **2025–2026**: **All courts** (local court, regional court) **ignored written evidence or rejected it**.
- **Consequence**: Those who commit to the constitutional order are **systematically hindered**.

Why the Judiciary Does Not Intervene

1. **No Identifiable Perpetrator**: With remotely controlled networks, there is no **natural person** as an attacker – or they act **unwittingly**.
2. **No Evidence**: Digital traces are **manipulable** or are **systematically suppressed**.
3. **No Legal Framework**: Existing laws are designed for **physical**, not **digital attacks**.
4. **No Self-Representation Without a Lawyer** before the regional court.
5. **Systemic Ignorance**: Courts **refuse to recognize patterns** or are **themselves remotely controlled**.

Solution Approaches

Approach 1: Technical Resilience Through EU-D-S

- **Measure**: **Closed, controlled systems** with **WAN-anonymous registration**.
  - **Trusted WEB 4.0**: All participants are **anonymous but traceable**.
  - **GISAD**: **Review** of all projects for **structural relevance**.
  - **De-Anonymization**: Only **in individual cases by court order**.
- **Advantages**:
  - **No single point of failure**.
  - Manipulation is **technically provable**.
  - **Protection against remote-controlled gang-like appearance**.
- **Disadvantages**:
  - **Closed system** – but this is **necessary for security**.
  - **No absolute anonymity** – but this is **necessary for justice**.

Approach 2: Legal Adjustments

- **Measure 1**: **Expansion of the Right to Resistance (Article 20(4) GG)**
  - **Current**: Resistance only against **physical** attacks on democracy.
  - **Proposal**: Expansion to **digital attacks and remote-controlled gang-like appearance**.
  - **Implementation**: Clear definition of "digital resistance" (e.g., use of EU-D-S for defense).
- **Measure 2**: **Right to Digital Self-Defense**
  - **Content**: Citizens may **actively** defend themselves against digital attacks.
  - **Examples**:
    - Use of **EU-D-S for documentation**.
    - Publication of evidence of manipulation **in protected systems**.
  - **Limits**: No **disproportionate** measures.
- **Measure 3**: **Anonymity Protection for Whistleblowers**
  - **Problem**: Currently, whistleblowers risk **criminal prosecution**.
  - **Solution**: **EU-D-S protects whistleblowers** through **technical anonymization**.

Approach 3: Societal Resilience

- **Measure 1**: **Digital Education as a Mandatory Subject**
  - **Content**:
    - Recognition of **remote-controlled gang-like appearance**.
    - Secure communication **within Trusted WEB 4.0**.
    - Legal options for digital attacks.
  - **Target Group**: **All citizens**, not just tech experts.
- **Measure 2**: **Civil Society Networks with getmySense**
  - **Task**: Monitoring and documentation of digital manipulation **with EU-D-S**.
  - **Examples**:
    - **Netzwerk Recherche** (investigative journalism).
    - **Digitalcourage** (data protection activism).
    - **Chaos Computer Club** (technical expertise).
  - **Advantage**: **Decentralized** defense, hard to attack.
- **Measure 3**: **Transparency Obligations for Algorithms**
  - **Problem**: Currently, algorithms (e.g., from social media) are **black boxes**.
  - **Solution**: **Disclosure obligation** for algorithms that influence **public opinion formation**.
  - **Implementation**: Expansion of the **Digital Services Act (DSA)** through **GISAD review**.

Comparison of Approaches

Approach	Effectiveness	Feasibility	Long-Term Benefit	Novelty
Technical Resilience (EU-D-S)	★★★★★	★★★★★	★★★★★	Closed System
Legal Adjustments	★★★★★★	★★	★★★★	Digital Right to Resistance
Societal Resilience	★★★	★★★★★	★★★★★	getmySense Integration

Recommendation: **Combination of all three approaches**, with priority on **technical resilience through EU-D-S** (immediate effect) and **societal education** (long-term resilience).

The Big Picture: A Genuine Digital Democracy with EU-D-S

Definition: Genuine Digital Democracy (with EU-D-S)

A digital democracy is **genuine** when:

1. **Technically**: Manipulation is **impossible** or at least **provable** (through EU-D-S).
2. **Legally**: Affected individuals receive **effective protection** (through expanded rights).
3. **Societally**: Citizens are **informed and capable of action** (through education).
4. **Politically**: Power **truly derives from the people** – not from algorithms or **remotely controlled actors**.
5. **Systemically**: **All structurally relevant projects** are reviewed by **GISAD**.

🎯 Part 3: Synthesis – Why There Is No Genuine Digital Democracy

---

The Five Structural Deficits

1. 🔓 **Technical Vulnerability**
   - Digital infrastructure is **not secured against manipulation**.
   - **Example**: GraTeach shows that **entire administrations can be remotely controlled**.
   - **All systems** (including expert opinions, courts) can be **manipulated**.
2. ⚖️ **Judicial Gaps**
   - Laws are designed for **physical**, not **digital attacks**.
   - **Example**: No criminal offense for "remote control of democracy" or "remote-controlled gang-like appearance".
   - **Judiciary itself can be part of the problem** (systemic ignorance).
3. 🏛️ **Political Ignorance**
   - Politicians **do not understand the threat** or **ignore it**.
   - **Example**: EU refers GraTeach to national justice – **knowing that it fails**.
   - **Politics uses mandatory legal representation as a tool of oppression**.
4. 👥 **Societal Naivety**
   - Citizens **underestimate** the threat of digital manipulation.
   - **Example**: Many believe, "this does not affect me".
   - **Citizens do not recognize remote-controlled gang-like appearance**.
5. 🌍 **Lack of International Cooperation**
   - Digital attacks are **cross-border** – national solutions are **inadequate**.
   - **Example**: Russia uses servers in **third countries** for attacks.
   - **EU-D-S can enable international cooperation technically**.

The Consequence: An Asymmetric War

Currently: Autocracies and remote-controlled gang-like appearance have the **upper hand** – democracies are on the **defensive**. **With EU-D-S**: The **power dynamics reverse** – democracies gain **defensive superiority**.

Why Autocracies Cannot Copy This

Feature	Democracy	Autocracy
Transparency	High (open society)	Low (censorship, secrecy)
Rule of Law	High (independent judiciary)	Low (judiciary as a tool of power)

Feature	Democracy	Autocracy
Civil Society	Strong (NGOs, media, activists)	Weak (suppressed)
Technological Dependence	High (open systems)	Low (closed systems)
Adaptability	High (innovation through freedom)	Low (rigid hierarchies)
Technical Infrastructure	**EU-D-S enables secure systems**	No comparable infrastructure

---

Conclusion: Autocracies **can** use digital manipulation techniques, but they **cannot build a genuine digital democracy** because the **foundations (EU-D-S, GISAD, Trusted WEB 4.0)** contradict their political approach.

🔮 Part 4: Trusted WEB 4.0 with GISAD and EU-D-S – The Game-Changer for Digital Democracy

---

4.0 Introduction: Why This Standard Would Change Everything

The introduction of **Trusted WEB 4.0** as a binding standard in the **EU Digital Space (EU-D-S)** as **technical infrastructure** would initiate a **paradigm shift**.

Trusted WEB 4.0 is the umbrella term for the patent applications by Olaf Berberich. **GISAD** is to be established as a solution to the problems identified in this study. Further information at www.gisad.eu. The technical infrastructure **EU-D-S** is provided by www.get-primus.com.

"Transparency is the natural enemy of manipulation. EU-D-S makes transparency technically possible – without new bureaucracy."

The legal basis can be found in the **EU-D-S Constitution**.

4.1 Definition: What Are Trusted WEB 4.0, GISAD, and EU-D-S?

Trusted WEB 4.0

- **Vision**: A **trustworthy, closed digital space** with **controlled anonymity**.
- **Principles**:
  - **Closed System**: All participants are **registered with WAN anonymity**.
  - **Controlled Transparency**: Projects with **societal structural relevance** must be disclosed.
  - **Traceability**: **De-anonymization** only possible in individual cases by **court order**.
  - **Security**: **By design** protected against manipulation.
- **Technical Basis**: Blockchain, end-to-end encryption, **EU-D-S infrastructure**.

GISAD *(Global Institute for Structure Relevance, Anonymity, and Decentralization)*

- **Status**: **To be established as a result of the identified problems**.
- **Task**: **Review** of all projects for **societal structural relevance**.
- **Website**: www.gisad.eu.

EU-D-S *(European Digital System)*

- **Task**: **Technical infrastructure** for Trusted WEB 4.0 – **not a bureaucracy, but a system**.
- **Functions**:
  1. **Automated Review**: All projects are reviewed for **societal structural relevance** (by GISAD).

2. **WAN-Anonymous Registration**: All participants are **anonymous but traceable**.
3. **De-Anonymization**: Only **in individual cases by court order**.
4. **Real-Time Monitoring**: **AI-supported detection** of manipulation attempts.

- **Advantage**: **No new bureaucracy** – EU-D-S is a **technical platform** that **protects by design**.
- **Website**: www.get-primus.com.

"Remote-controlled gang-like appearance has nothing to do with decentralized networks. Whoever has sufficient information about the entire environment can disable or control anyone without them recognizing the connection. The only solution is that everyone can be de-anonymized in individual cases by court order."

4.2 The Five Systemic Effects of Trusted WEB 4.0 + GISAD + EU-D-S

◇ Effect 1: The End of Digital Anonymity for Manipulators

Aspect	Before	After
Project Development	Secret	**GISAD review for structural relevance**
Participant Identity	Anonymous/faked	**WAN-anonymous, but traceable**
Manipulation Attempts	Undetected	**Real-time detection by EU-D-S**
Evidence	Manipulable	**Technically secured by EU-D-S**

Consequences:

- **Early warning system** for democracy-endangering technologies.
- **Provability** of manipulation through **technical documentation**.
- **Deterrence** through **traceability**.

◇ Effect 2: The Judiciary Finally Gets Tools Against Remote-Controlled Gang-Like Appearance

Current Blockades (GraTeach Example):

1. **No Evidence**: All documents were **manipulated or suppressed**.
2. **No Responsible Parties**: All actors acted **unwittingly** or **remotely controlled**.
3. **No Prevention**: Judiciary can only act **after** damage occurs – if at all.

With Trusted WEB 4.0 / GISAD / EU-D-S:

Specific Improvements:

- **Preventive Interventions**: Courts can act **before** damage occurs if GISAD reports a **structural threat**.

- **Automated Evidence Collection**: **All activities** in Trusted WEB 4.0 are **technically documented**.
- **De-Anonymization**: If suspected, judges can **specifically de-anonymize participants**.
- **EU-Wide Enforcement**: **EU-D-S operates cross-border** – without new bureaucracy.

◇ **Effect 3: Civil Society and Media Gain Superpowers**

Actor	New Capabilities
NGOs	Systematic review of all **GISAD-approved projects**
Media	Access to **EU-D-S documentation** of manipulation attempts
Science	Empirical research based on **EU-D-S data**
Citizens	**Secure communication** within Trusted WEB 4.0
Whistleblowers	**Technical protection** through EU-D-S anonymization

Emerging Ecosystems:

1. **Transparency Platforms**: Independent portals aggregating and analyzing **EU-D-S data**.
2. **getmySense**: Citizen participation platform with EU-D-S support (replaces citizen councils).
3. **AI Watchdogs**: Algorithms **automatically** searching for manipulation patterns in EU-D-S data.
4. **European Digital Cooperatives**: Citizens operate **their own EU-D-S-protected** digital infrastructure.

◇ **Effect 4: Remote-Controlled Gang-Like Appearance Loses Its Power**

- **Currently**: Remotely controlled actors act **unwittingly** – the **central intelligence** is **not identifiable**.
- **With EU-D-S**:
  - **All activities are documented**: **Technical evidence** can no longer be suppressed.
  - **Central intelligence becomes visible**: Through **pattern recognition in EU-D-S**, the **controlling entity** can be identified.
  - **Remotely controlled actors are exposed**: **De-anonymization** shows who was **actually controlled**.

◇ **Effect 5: The Economy Becomes an Ally of Democracy**

Incentive	Description
Compliance Bonuses	Companies that are **GISAD-compliant** receive **tax benefits**.

Incentive	Description
Democracy Bonus	Projects with **positive societal impact** are **state-funded**.
Reputation Gain	**"GISAD-certified"** becomes a **quality seal**.
Market Access	Only companies with **GISAD certification** can participate in **public tenders** in EU-D-S.

Emerging Business Models:

1. **GISAD Consulting**: Companies helping others become **GISAD-compliant**.
2. **Transparency Technologies**: Tools for **automated EU-D-S registration**.
3. **Security Audits**: Independent review of **democracy-endangering risks** by GISAD.
4. **Citizen Participation Platforms**: Companies enabling **EU-D-S-protected participation**.

4.3 Opportunities and Risks in Detail

☑ Opportunities

Opportunity	Description	Likelihood	Impact
End of Digital Helplessness	Judiciary and civil society get **tools** against manipulation	★★★★★	★★★★★
Preventive Defense	Democracy-endangering projects are **stopped before** market introduction	★★★★	★★★★★
Power Shift	From remotely controlled networks to **citizens and NGOs**	★★★★	★★★★
Innovation Boost	Companies develop **democracy-friendly** technologies	★★★	★★★★

❌ Risks

Risk	Description	Likelihood	Impact	Countermeasure
Surveillance State	EU-D-S is misused for **mass surveillance**	★★	★★★★	**Strict judicial control**
Technical Errors	EU-D-S detects **false patterns**	★★★	★★★	**Human review**
Evasion Attempts	Companies **disguise** their projects	★★★★	★★★	**AI-supported detection**
Acceptance Issues	Citizens reject **closed systems**	★★★	★★★★	**Education about benefits**
Costs	Building EU-D-S is **expensive**	★★★	★★	**EU-wide financing**

4.4 Concrete Implementation: The Roadmap to Trusted WEB 4.0 with GISAD and EU-D-S

Phase	Timeframe	Measures
Phase 1: Preparation (2026–2027)	2026–2027	'- Development of **EU-D-S infrastructure** by www.get-primus.com. - **Legal Basis**: EU regulation for **mandatory GISAD review of structurally relevant projects**. - **Pilot Projects**: Voluntary participation of **100 companies**. - **Public Relations**: Education about the **benefits of Trusted WEB 4.0**. - **Founding of GISAD**: www.gisad.eu.
Phase 2: Introduction (2028–2030)	2028–2030	'- **Certification System**: **"GISAD-certified"** seal for compliant companies. - **Citizen Participation**: Introduction of **getmySense** with EU-D-S support. - **Whistleblower System**: **WAN-anonymous reporting platform** with EU-D-S protection.
Phase 3: Full Implementation (2030–2035)	2030–2035	'- **Widespread Acceptance**: All companies recognize the benefits and participate. - **AI Monitoring**: **Automated detection** of manipulation attempts. - **Global Expansion**: **Cooperation with USA, Japan, South Korea** for worldwide standard. - **Democracy Index**: **Annual evaluation** of digital democracy quality in the EU.

4.5 Trusted WEB 4.0 with GISAD and EU-D-S and the Five Research Questions

Research Question	Solution Through Trusted WEB 4.0 + GISAD + EU-D-S
Q1: Judicial Self-Commitment vs. Protection Against Public Harm	**EU-D-S makes the judiciary an active designer**: Preventive interventions, automated evidence collection, targeted de-anonymization.
Q2: EU-Wide Obligation to Act	**EU-D-S makes the EU a global pioneer – without new bureaucracy**: Technical infrastructure, automatic coordination, sanctions.
Q3: "All State Authority Derives from the People"	**EU-D-S returns power to citizens**: Participation, transparency, control through getmySense and NGOs.
Q4: What Is Remote-Controlled Gang-Like Appearance?	**GISAD makes it visible and provable**: Pattern recognition, identification of central intelligence, provability.
Q5: How Can Trusted WEB 4.0 Solve the Problem?	**EU-D-S and GISAD are the technical solution**: Closed system, no new bureaucracy, judicial control.

4.6 Conclusion: Why Trusted WEB 4.0 with GISAD and EU-D-S Is the Only Way Out

The Historic Opportunity

Trusted WEB 4.0 + GISAD + EU-D-S is **not a utopia, but the only realistic solution** to the problems identified in this study. The alternative is:

- **Continuation of the status quo**: Democracies remain **vulnerable** to digital attacks and remote-controlled gang-like appearance.
- **Autocratic Dominance**: China, Russia & Co. **dominate** the digital future.
- **Collapse of the Rule of Law**: Judiciary and politics **lose control** over technology.

GISAD is to be established as a solution to these problems. More information at www.gisad.eu.

The Vision: A Genuine Digital Democracy with GISAD and EU-D-S

With Trusted WEB 4.0, GISAD, and EU-D-S, the EU becomes the **global beacon** for:

☑ **Technical Security**: Manipulation is **impossible** or at least **provable** (through EU-D-S).
☑ **Legal Protection**: Affected individuals receive **effective protection** (through expanded rights).

☑ **Political Capability**: The EU and member states **cooperate technically** (through EU-D-S).

☑ **Societal Resilience**: Citizens are **informed and capable of action** (through EU-D-S data).

☑ **Systemic Integrity**: **Remote-controlled gang-like appearance** becomes **visible, provable, and combatable**.

"Trusted WEB 4.0 with GISAD and EU-D-S is not just a technical standard – it is the salvation of democracy in the digital age. And the best part: It works without new bureaucracy, purely through intelligent technology that protects democracy instead of monitoring it."

🚀 Part 5: Recommendations for Action – The Path to a Genuine Digital Democracy

Note: The following measures complement the structural reforms described in Part 4 (Trusted WEB 4.0 + GISAD + EU-D-S).

Short-Term Measures (0–2 Years)

Measure	Content	Implementation	Cost
Emergency Plan for Digital Attacks	Clear **instructions** for authorities in case of digital manipulation	Nationwide **cyber emergency center with EU-D-S connection**	~€50 million/year
Expansion of the Right to Resistance	Art. 20(4) GG expanded to include **digital attacks and remote-controlled gang-like appearance**	Constitutional amendment or **broad interpretation** by the Federal Constitutional Court	–
Immediate Introduction of Trusted WEB 4.0 Pilot Projects	Testing **GISAD in closed systems**	**40 companies** (EU-D-S founders)	–

Medium-Term Measures (2–5 Years)

Measure	Content	Cost
Securing Technical Infrastructure	**State-funded EU-D-S infrastructure** by www.get-primus.com	~€200 million/year
Adapting the Legal Framework	'- **New criminal offense**: "Digital manipulation of democratic processes through remote-controlled gang-like appearance". - **Expansion of legal aid** to **lawsuits with GISAD confirmation**. - **Immunity for digital whistleblowers** – **EU-D-S protects identity**.	–
Public Awareness	**Mandatory subject "Digital Competence and EU-D-S Usage"** in schools and vocational training	~€100 million/year

Long-Term Measures (5–10 Years)

Measure	Content	Goal
European Digital Constitution with GISAD	Fundamental rights for the digital age **technically secured by EU-D-S**	EU treaty amendment + **GISAD integration**
Global Cooperation	**UN Convention against digital manipulation** with **EU-D-S standard**	**Prohibition** of digital attacks on democratic processes
Technological Sovereignty	**European alternatives** to US and Chinese tech giants **with EU-D-S integration**	**Independence** from external actors

Part 6: Sources and References

Primary Sources

Source	Type	Credibility	Last Updated	Relevance
Letter to the President of the Court (File No. 3132-1582)	Court documents	5/5	03.09.2026	**Central evidence for remote-controlled gang-like appearance**
Finders: Digital Autocracy and Censorship Are Remote-Controlled Gang-Like Appearance Today	Analysis	5/5	2026	**Definition and analysis**
EU-D-S Constitution	Constitution	5/5	2025	**Legal basis**
Finders Archive: Year Search	Document collection	5/5	2026	**Additional evidence**
Federal Constitutional Court: Rulings on Art. 20 GG	Case law	5/5	2026	**Legal basis**
EU Commission: Digital Services Act	Law	5/5	2024	**Regulatory framework**
Chaos Computer Club: Reports on Digital Security	NGO report	4/5	2026	**Technical expertise**
Netzwerk Recherche: Investigative Journalism	Journalism	4/5	2026	**Investigations into manipulation**
GISAD: Global Infrastructure for Secure and Accountable Democracy	Initiative (in founding)	4/5	2026	**Technical solution**
EU-D-S: European Digital System	Infrastructure	4/5	2026	**Technical platform**

Secondary Literature

Author	Title	Year	Credibility	Relevance
Shoshana Zuboff	"The Age of Surveillance Capitalism"	2019	5/5	Surveillance capitalism
Timothy Snyder	"On Tyranny: Twenty Lessons from the Twentieth Century"	2017	5/5	Autocracy research
Marietje Schaake	"The End of Big Tech: How to Restore Our Democracy"	2023	4/5	Tech regulation

Author	Title	Year	Credibility	Relevance
Bruce Schneier	"Click Here to Kill Everybody: Security and Survival in a Hyper-connected World"	2018	5/5	Digital security
Evgeny Morozov	"The Net Delusion: The Dark Side of Internet Freedom"	2011	4/5	Digital manipulation

---

Own Material

Document	Type	Date	Relevance
Application to Regional Court	Court application	03.09.2026	**Central evidence**
GraTeach Criminal Proceedings	Case documentation	2001–2009	**Remote-controlled gang-like appearance**
WEG Proceedings	Case documentation	2023–2026	**Systematic obstruction**

💡 Part 7: Open Questions and Further Research

Unanswered Questions

1. **Technical Feasibility**
   - How can **EU-D-S** be designed to be **user-friendly**?
   - Are there **technical solutions** that **completely prevent manipulation**?
   - How can **WAN-anonymous registration** be implemented **securely and in a data-protection-friendly way**?
2. **Legal Limits**
   - How can the **right to resistance** be concretely applied to **digital attacks and remote-controlled gang-like appearance**?
   - Where is the line between **legitimate self-defense** and **illegal hacking**?
   - How can **de-anonymization** be **judicially controlled** without enabling **mass surveillance**?
3. **Political Feasibility**
   - How can the **political will** for EU-D-S and GISAD be generated?
   - How to prevent **lobbying** (e.g., by tech giants) from blocking implementation?
   - How can **EU-D-S be introduced without new bureaucracy**?
4. **Societal Acceptance**
   - How can the **public** be sensitized to the **necessity of closed systems**?
   - How to avoid **paranoia** and **loss of trust** in digital systems?
   - How can **EU-D-S be marketed as a protective tool, not a surveillance instrument**?

Research Proposals

1. **Empirical Studies**
   - **Survey**: How many citizens have already been victims of **remote-controlled gang-like appearance**?
   - **Experiment**: How effective are **awareness campaigns about EU-D-S**?
2. **Technical Analyses**
   - **Security Audits**: Review of **EU-D-S for vulnerability to manipulation**.
   - **AI-Supported Detection**: Development of tools for **automated detection of remote-controlled gang-like appearance**.
3. **Comparative Legal Studies**
   - **Best Practices**: Which countries have **successful models** for defending against remote-controlled gang-like appearance?
   - **Legal Gap Analysis**: Where exactly do current laws fail with **remotely controlled attacks**?
4. **Scenario Analyses**
   - **Future Scenarios**: How could a **genuine digital democracy with EU-D-S** look in 10, 20, 50 years?
   - **Risk Analyses**: What **new threats** could arise from EU-D-S?

🎯 Part 8: Conclusion – The Urgent Need for Action

The Central Insight

There is currently no genuine digital democracy – but with Trusted WEB 4.0, GISAD, and EU-D-S, it can become a reality.

Current structures enable autocratic actors, organized networks, and **remotely controlled gang-like structures** to systematically undermine democratic systems **without the rule of law being able to effectively counter them**. The cases **GraTeach**, **criminal proceedings (anonymized)**, and **WEG proceedings (anonymized)** show:

1. **The threat is real** – and it is happening **now**.
2. **The judiciary is overwhelmed** – and has **no tools** to act.
3. **Politics ignores the problem** – or **does not understand it**.
4. **Society is unaware** – and thus **vulnerable**.
5. **Remote-controlled gang-like appearance is feasible** – and **works perfectly** in democratic systems.

But there is a way out: Trusted WEB 4.0 with GISAD and EU-D-S.

The Appeal

To Politicians

- **Act now!** The next 2–3 years are **decisive**.
- **Introduce EU-D-S** – **without new bureaucracy**, purely as **technical infrastructure**.
- **Give the judiciary the tools** it needs: **De-anonymization by court order**.
- **Protect citizens** from remote-controlled gang-like appearance through **Trusted WEB 4.0**.

To the Judiciary

- **Recognize your responsibility** – not just for individuals, but for the **system**.
- **Use EU-D-S** as a **tool to uncover manipulation**.
- **Acknowledge remote-controlled gang-like appearance** – it is **real and provable**.
- **Allow written proceedings** – they are the **only defense against remotely controlled attacks**.

To Civil Society

- **Educate yourselves** – digital competence and **EU-D-S usage** are **survival skills**.
- **Organize yourselves** – only together can you defend against **remote-controlled gang-like appearance**.

- **Use Trusted WEB 4.0** – it is your **only secure communication platform**.

To Every Individual

- **Stay vigilant** – question what you see online.
- **Protect yourselves** – use **Trusted WEB 4.0 and EU-D-S**.
- **Engage yourselves** – democracy is not self-sustaining, **especially not in the digital age**.

The Vision

A **genuine digital democracy** is possible – but only if we **act now**. With **Trusted WEB 4.0, GISAD, and EU-D-S**, it would be characterized by:

☑ **Technical Security**: Manipulation is **impossible** or at least **provable** (through EU-D-S). ☑ **Legal Protection**: Affected individuals receive **effective help** (through expanded rights and EU-D-S). ☑ **Political Capability**: The EU and member states **cooperate technically** (through EU-D-S). ☑ **Societal Resilience**: Citizens are **informed and capable of action** (through EU-D-S data). ☑ **Systemic Integrity**: **Remote-controlled gang-like appearance** becomes **visible, provable, and combatable**.

"The best time to build a genuine digital democracy was 20 years ago. The second-best time is now – with Trusted WEB 4.0, GISAD, and EU-D-S. And the best part: It works without new bureaucracy, purely through intelligent technology that protects democracy instead of monitoring it."

This study is continuously updated. For questions, suggestions, or additions, please contact the author.

Special thanks to all those who, through their work and their silence, made this study possible.

Impressum / Legal Notice
DE
Global Institute for Structure relevance,
Anonymity and Decentralization i.G.

Initiator
Olaf Berberich

Breiten Dyk 14
47803 Krefeld
Telefon : 02151-3872601
Mail: infoh@finders.de
Web: www.gisad.eu
EU-Register Nr. **244298340978-40**

Complainant at the Federal Constitutional Court:
- 1 BvR 227/23 - , -1 BvR 1640/24-, -1 BvR 1641/24-,
-2 BvR 907/24 -, -1 BvR 1426/25 -, -2 BvR 1668/25-
-1 BvR 91/26 -

Datenschutz

Die Texte der Studien basieren auf automatischen Recherchen im Internet und werden mithilfe der KI Mistral.ai optimiert und übersetzt. Dabei werden Quellen automatisch ermittelt. Alle Angaben werden sorgfältig geprüft. Sollte sich im Einzelfall doch einmal ein Fehler einschleichen, wären wir für jeden Hinweis dankbar.
Bitte beachten Sie dass von facebook.de, WhatsUp und weiteren Portalen Accounts unter meinem Namen angelegt sind, welche ich nicht pflege, aber auch nicht löschen kann. Außer über E-Mail können Sie GISAD über XING oder Linkedin erreichen!

GISAD für ein starkes digitales Europa!
Mit Hilfe der EU die vordigitalen Errungenschaften erhalten!

GISAD