

SAFEGUARDING DEMOCRACY & ELECTIONS IN THE AGE OF AI

CHALLENGES

AI is reshaping how citizens participate, access information & engage politically, **creating new opportunities** for democracy **while also amplifying** manipulation, (algorithmic) bias, surveillance, over-reliance & coordinated influence operations **that threaten** trust, information integrity & democratic freedoms.

AI can:

- ✓ Increase Info Access & Awareness
- ✓ Expand Participation
- ✓ Improve Transparency
- ✓ Boost Accountability
- ✓ Innovate Civic Engagement

AI - A DUAL PATH

BUT AI can also:

- ✗ Amplify & Weaponize Grievances & Polarisation
- ✗ Pollute Information ("*Liar's Dividend*" where *authentic content is dismissed as fake*)
- ✗ Concentrate Power, Surveillance & Censorship
- ✗ Automate Discrimination, Violence & Divisiveness
- ✗ Outpace Oversight (Acceleration & Scale)

WHAT'S AT STAKE



Electoral Integrity. Distinguish fact from fiction, gain awareness & resist foreign interference.



Democratic Sovereignty & Regulation. "The Democracy Shield." No one-size-fits-all regulatory models, be rights-based, context-sensitive & local. Inclusive rule-setting.



AI Governance & Platform Accountability. Oversee AI systems & political influence operations. Who responsible?



Civic Space & Digital Participation. Keep online civic spaces open, inclusive, safe & resilient.



Information Integrity & Evidence-based Public Debate. Centralise digital literacy & education.



Public Trust & Protection of Rights. Balance freedom of expression, privacy & control.

COUNTRY CASE STUDIES & PRACTICES

1

Civic Innovation & Democratic Participation

Taiwan

"Pol.is/Polis" digital participation platform → Digital space for civic dialogue, consensus-building & policy co-creation through large-scale digital engagement.

Kenya

AI chatbot "Finance Bill GPT" & "Corruption Tracker" → AI tools helping citizens understand the 2024 bill, detect corruption & monitor public accountability.

Brazil

"Open Knowledge" initiatives → Open data approaches strengthening transparency & oversight.

2

Election Integrity & Information Resilience

Mexico

National Electoral Institute (INE) five-pillar model → Combines fact-checking hubs, verification chatbots, platform cooperation & nationwide media literacy campaigns. "Soy Digital."

South Africa

Multi-stakeholder election integrity framework → Collaborative ecosystem = Electoral Commission, civil society, media & technology platforms working together through verification & early-warning systems. (*Involved Google, Meta, TikTok & Media Monitoring Africa, alongside AI tools like Real411 for complaints, Africa Check & the Google News Initiative*).

3

Disinformation, Influence & Political Manipulation

Bangladesh

State-supported online influence networks → Coordinated manipulation, fake "experts" & censorship undermining democratic debate.

Ghana

Coordinated hashtag campaigns & paid influencers to spread divisive messages esp. vs. LGBTQIA+ communities → Polarisation & targeted information manipulation.

Indonesia

AI-driven political branding, deepfakes & professionalised "buzzer" networks (digital operatives – ideological or commercial) → Demonstrates how AI amplifies digital propaganda & influence operations.

Pakistan

AI-generated political messaging & synthetic content → Highlights both the risks & political adaptability of generative AI.

4

Rights-Based Governance & Regulation

Indonesia

AI governance & regulatory debates → Illustrates the risks of censorship, weak safeguards & regulatory models not adapted to local contexts (linguistical & remoteness).

Global Governance Initiatives

"UN Global Digital Compact," "Paris AI Action Summit" & emerging national frameworks → Demonstrate growing efforts to establish democratic guardrails for AI governance.

APPROACHES & TAKEAWAYS FOR TEAM EUROPE



AI governance should be anchored in international human rights law, locally owned & context-sensitive, applied across the full AI lifecycle (design, deployment, oversight), strengthened through South–South cooperation & peer learning rather than replication of external regulatory frameworks, as it is **not a one-size-fits-all model**.



Whole-of-society implementation ecosystems & cross-institutional collaboration involving election authorities, civil society, independent media, academia, law enforcement, courts, influencers & technology platforms are important to detect, verify & respond to information threats, with clear roles for stakeholders involved & data protection authorities in setting enforceable standards.



Citizens are active participants in AI governance, not passive consumers. Strengthening civic education, digital literacy, independent journalism & local fact-checking is central to rebuilding trust & making inclusion operational rather than symbolic, with a focus on youth, women & marginalised communities.



Beyond regulatory compliance, AI governance requires sustained (long-term) investment in institutional capacity, transparency, innovation & trust. This includes strengthening independent institutions & oversight capacities, embedding data protection & enforcement mechanisms & **addressing structural drivers of disinformation** such as inequality, polarisation & weak accountability.