AI IN THE DEMOCRATIC SPHERE AND THE ELECTORAL PROCESS

Abstract: The rapid development of artificial intelligence has now reached a stage where generative AI is both powerful and accessible enough to be used at scale in election campaigns, at least in principle. The scope and purpose of this study is to highlight the various ways in which AI has been and is being utilised in election campaigns. It will firstly examine the darker dimensions of AI in electoral processes such as algorithmic bias, deep-fake videos, the spread of fake news, and the increasing threat of foreign interference in local elections. Subsequently, it will analyse the manner in which democratic societies, public institutions and legal frameworks can respond to these challenges, such as the through the AI Act. Moreover, the study will seek to provide data on how AI mechanisms are used to influence voters and overall public opinion. Additionally, based on the available research, the study will highlight adequate pathways for the EU to build resilience against misinformation and the safeguarding of our democratic rights and values. Finally, it will assess emerging challenges regarding AI regulation when it comes to issues such as transparency, accountability and informed consent and decision-making.

Table of Contents

Introduction: AI's recent use in political affairs

The rapid advances in artificial intelligence (AI) have been raising questions and unprecedented challenges to democratic institutions, relations between state and society and to democracy itself. AI is a general-purpose technology which impacts almost all technological, financial and communication sectors.[1] The very nature of AI is also altering how power is exercised and maintained by influencing the social and psychological levers that maintain and bolster such power. These changes in our society, which have most recently tampered with global electoral processes, are now directly impacting governance across the world. Additionally, governmental use of AI to amplify control over their societies and data produce exceptional challenges on human rights and fundamental freedoms.

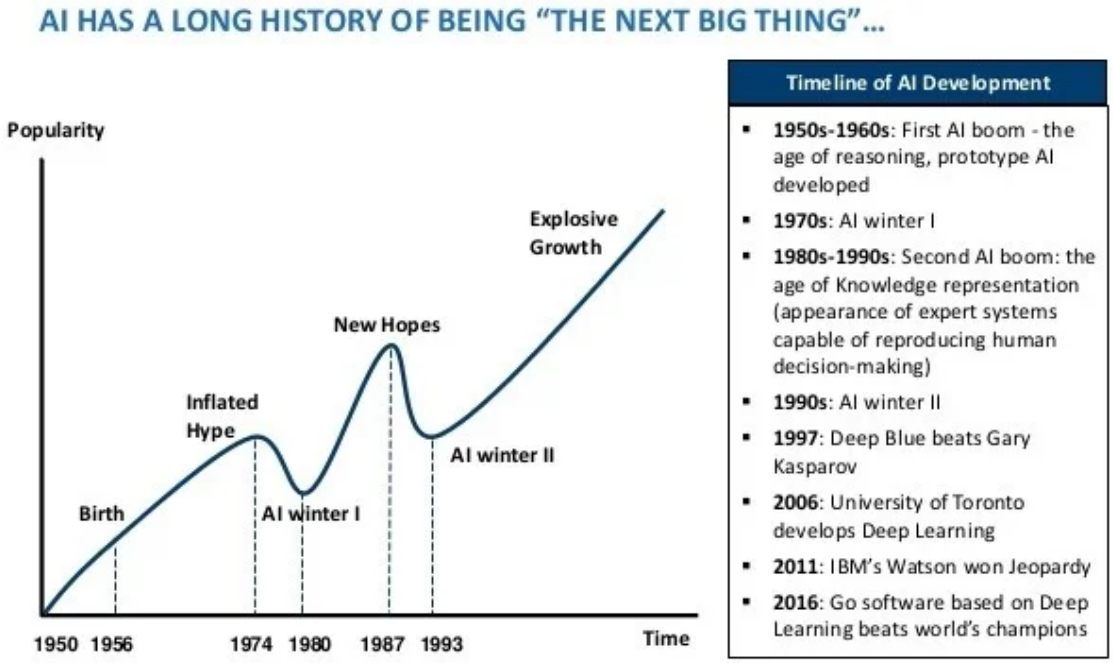
AI and algorithms offer governments' unmatched capabilities to sift through vast amounts of data quickly. That being said, AI has now transformed itself into a mainstay in civil society, nevertheless, its impact is two-fold. Most authoritarian governments have shifted their focus away from merely collecting big data', defined as the volume of information not processable by standard computer hardware or storage infrastructures, too fathoming and interpreting what is contained therein. For an authoritarian regime, this means identifying patterns of dissent, potential threats, or even understanding public sentiment to a granularity that was previously unimaginable.[2]

Though there are questions about the extent to which AI-generated tools affect voters, at the same time there is an increasing number of examples of how campaigns use AI and Large Language Models (LLM). The range of how these tools are being used in electoral processes spans from personalised fundraising emails, a practice common in the US and the EU elections, to generated videos of candidates making personal appeals to voters.[3]

This study will analyse the darker dimension of AI which transpires in the form deep-fakes, algorithmic bias and the increasing foreign interreference in local elections. We will aim to understand how the darker dimension of AI is affecting voters and the broader civil society before moving on to discuss the ways in which we can safeguard democratic values and institutions from these darker dimensions. **More specifically the main question that we will discuss is how we can strategically build resilience moving into the future.**

[1] https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf
[2] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331635
[3] https://www.nytimes.com/2024/04/18/world/asia/india-election-ai.html

Artificial Intelligence: A Brief Background



Artificial Intelligence (AI) has roots stretching back centuries in myth, philosophy and early logic, but it genuinely took shape in the mid-20th century. In his landmark 1950 paper "Computing Machinery and Intelligence," Alan Turing posed the question "Can machines think?" and introduced what we now call the **Turing Test**, conjecturing that if a machine could convincingly imitate a human in conversation, it would be considered intelligent.[4] The term **"**artificial intelligence" was coined in 1956 at the Dartmouth Summer Research Project, organised by John McCarthy, Marvin Minsky, Nathaniel Rochester and Claude Shannon.

The following decades saw cycles of optimism and disillusionment. Early successes in programming and logic were followed by funding cuts and critical reports that sparked the first **"AI Winter"** in the 1970s.[5] But research persisted, and by the early 2000s, the combination of big data, more powerful hardware and machine learning techniques, especially deep neural networks brought about breakthroughs in image recognition, natural language processing and generative AI. The revival accelerated after 2012, culminating in transformer-based architectures and widely used large LLM's.

Today AI is increasingly prominent in healthcare, finance, transport, and politics, even as experts warn of challenges like bias, interpretability, and a mounting impact on civil society.

[4] https://st.llnl.gov/news/look-back/birth-artificial-intelligence-ai-research?utm_source=chatgpt.com
[5] https://www.historyofdatascience.com/ai-winter-the-highs-and-lows-of-artificial-intelligence/

Key Definitions

AI literacy: refers to the ability to understand, use, evaluate, and critically engage with artificial intelligence technologies. It involves knowledge of how AI works, its potential benefits, limitations, and societal impacts, enabling informed decision-making in an AI-driven world.

Microtargeting: is a marketing and political strategy that uses data analytics too deliver highly personalized messages or advertisements to specific groups or individuals based on their demographics, interests, behaviours, and online activity. It aims to influence decision-making by tailoring content to the unique preferences of each audience segment.

AI powered chatbots: are software applications that use artificial intelligence, particularly natural language processing (NLP) and machine learning, to simulate human-like conversations. They can understand, interpret, and respond to user queries in real time, often used for customer service, virtual assistance, and information retrieval.

Deep fakes: are synthetic media, typically images, audio, or videos, crafted or altered using artificial intelligence techniques, such as deep learning, to convincingly mimic real people or events. They can be used for entertainment, satire, or malicious purposes like misinformation and fraud.

Disinformation: is false or misleading information that is deliberately created and spread with the intention of deceiving or manipulating people. It is often used to influence public opinion, obscure the truth, or achieve political, financial, or social goals.

Misinformation: is false or inaccurate information that is shared or spread without the intent to deceive. Unlike disinformation, it is often the result of misunderstanding, rumour, or lack of fact-checking.

Transparency: refers to the practice of openly sharing information, processes, and decision-making criteria, allowing others to understand how and why actions are taken. In technology and AI, it often means making systems, data use, and algorithms clear and accessible to promote trust and accountability.

Regulation: is the establishment of rules, laws, or guidelines created by governments or authoritative bodies too control or manage activities within a specific sector. In the context of technology and AI, regulation aims to ensure safety, fairness, privacy protection, and ethical use of these systems.

Ethics: refers to the principles and moral values that guide human behavior and decision-making, determining what is right or wrong. In AI and technology, ethics involves ensuring that developments and applications respect fairness, privacy, accountability, and the well-being of individuals and society.

General-purpose AI (GPAI) models: perform a wide range of tasks and are becoming the basis for many AI systems in the EU. Some of these models could carry systemic risks if they are very capable or widely used.

Regulatory sandboxes: generally refer to regulatory tools allowing businesses to test and experiment with new and innovative products, services or businesses under supervision of a regulator for a limited period of time. As such, regulatory sandboxes have a double role: 1) they foster business learning, i.e. the development and testing of innovations in a real-world environment; and 2) support regulatory learning, i.e. the formulation of experimental legal regimes to guide and support businesses in their innovation activities under the supervision of a regulatory authority.

Legal Frameworks

Digital Services Act (DSA): The Digital Services Act aims to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. The set of rules of the DSA apply throughout the entirety of the EU. It aims to create a safer digital space in which the fundamental rights of all users of digital services are protected.[6]

AI Pact: The AI Act entered into force on 1 August 2024. While certain provisions already apply, others—particularly those concerning high-risk AI systems—will only take effect after a transitional period between the Act's entry into force and its full applicability. To support stakeholders in preparing for implementation, the European Commission has launched the *AI Pact*, which is built around two main pillars.[7]

AI Act: The Artificial Intelligence Act is a European Union regulation concerning artificial intelligence. It establishes a common regulatory and legal framework for AI within the European Union. It came into force on 1 August 2024, with provisions that shall come into operation gradually over the following 6 to 36 months.

What is the AI Act?

Key Points

- The law aims to protect citizens' fundamental rights.
- It also aims to harmonize the EU market by creating uniform rules for AI.
- It is expected to have a significant global impact, potentially influencing AI regulations worldwide and establishing a benchmark for ethical AI development.
- The Act also holds various actors in the AI supply chain accountable.

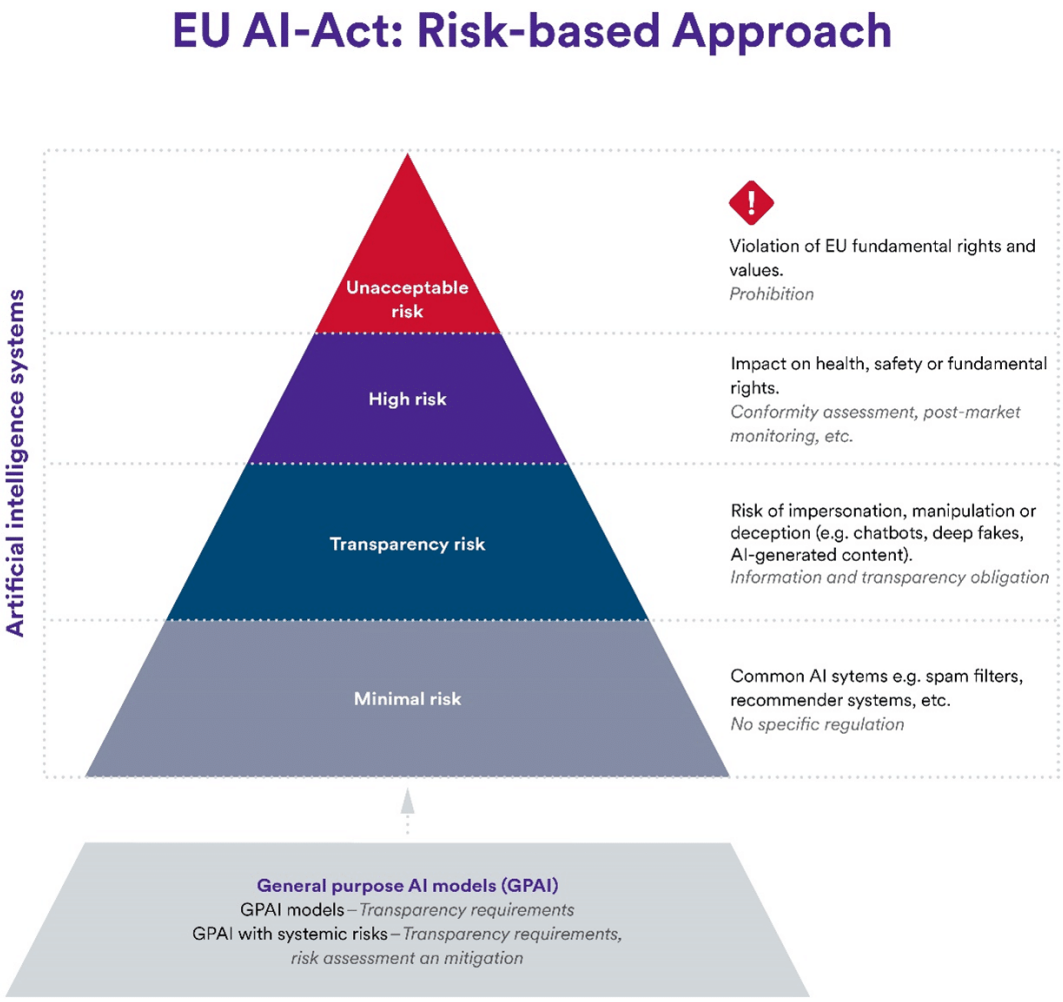
As part of its digital strategy, the EU wanted to regulate artificial intelligence to ensure better conditions for the development and use of this innovative technology.[8] AI can create many benefits, in the fields of cleaner transport, manufacturing, healthcare and sustainable energy, however, when it comes to its impact on the political stage AI tools have been contesting legislations, freedom of expression, and human rights.

From 2021 the European Parliament set as a priority to ensure that AI systems used in the EU will be transparent, safe, traceable, non-discriminatory and environmentally friendly. In order to do so the Parliament expected that AI systems should be overseen by people, rather than by automation, and in this way, it would attempt to prevent harmful outcomes by establishing the world's first comprehensive law regulating AI.

The Act applies rules based on the potential harm an AI system could cause. AI systems that can be used in different applications are analysed and classified according to the risk they pose

[6] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[7] https://digital-strategy.ec.europa.eu/en/policies/ai-pact
[8] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#ai-regulation-in-europe-the-first-comprehensive-framework-4

to users. The different risk levels mean more or less AI compliance requirements.[9] Although most AI systems pose minimal risk, there still needs to be a risk assessment, as demonstrated through the Act's risk-based classification system.



European Parlimanet: Artificial intelligence act, europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

In June of 2024, the EU AI Act adopted the world's first rules on AI, which will be fully applicable 24 months after entry into force with the exceptions of: .

1. The ban on AI systems posing unacceptable risks which came in to force on the 2nd of February 2025.

2. The codes and practice which was applied in March 2025.

3. The rules on general purpose AI systems that need to comply with transparency requirements which came into force in June 2025.

[9] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#ai-regulation-in-europe-the-first-comprehensive-framework-4

Government-purpose AI (GPAI) models

In July of 2025, the European Commission introduced 3 key instruments to support the responsible development of GPAI models.

1. The guidelines on the scope of the obligations for providers of GPAI models clarify the scope of the GPAI obligations under the AI Act, helping actors along the AI value chain understand who must comply with these obligations.

2. The GPAI Code of Practice is a voluntary compliance tool submitted to the Commission by independent experts, which offers practical guidance to help providers comply with their obligations under the AI Act related to transparency, copyright, and safety & security.

3. The template for the public summary of training content of GPAI models requires providers to give an overview of the data used to train their models. This includes the sources from which the data was obtained (comprising large datasets and top domain names). The template also requests information about data processing aspects to enable parties with legitimate interests to exercise their rights under EU law.

The purpose of these tools is to work in unison in order to provide a clear and actionable framework for GPAI providers in order to comply with the AI Act. In turn they look to reduce administrative burden and foster innovation while safeguarding fundamental rights and public trust.

AI regulations are prioritising a controlled use of AI and one which will aim to gain the trust of the civil society in order to safely implement it in daily use. A 2022 European Parliament report argued for "a favourable regulatory environment, including dynamic law-making and modern governance, as current EU and national legislation are fragmented, slow and do not provide legal certainty. To support innovation and avoid regulatory burden, only high-risk AI applications should be strictly regulated." Additionally, "the EU should support the development of AI skills so that people have the skills needed for life and work. This will also help create trust in the technology, foster innovation and, by supporting excellence centres and EU experts, prevent a brain drain.[10]

AI regulation therefore is being put into force in order to facilitate a human existence whereby AI has structured control over decision making (at all levels) rather than taking over spheres of influence, something which will be examined below as we delve into AI's darker dimensions.

However more recently Dr. Mario Draghi has been urging the EU to loosen its strict privacy rules (like GDPR) and pause parts of the new AI Act that regulate "high-risk" systems. He believes the current rules are too heavy and complex, making it hard for European companies to innovate and compete globally. Draghi's goal is to simplify regulations so businesses can

[10] https://www.europarl.europa.eu/topics/en/article/20220422STO27705/the-future-of-ai-the-parliament-s-roadmap-for-the-eu

develop AI more freely, while critics warn this could weaken privacy and safety protections for citizens.[11]

AI's current role in elections: Darker dimension of AI in electoral processes *(Deep-fakes, Algorithmic bias, Foreign interference)*

2024 has been the largest year for elections in human history with a total of 3.7 billion eligible voters in 72 countries who had the chance to go to the polls.[12] However, the most important element of these elections was that they were the first AI elections, where deepfakes and AI-generated misinformation overwhelmed the democratic processes. While AI did not play as big a role as anticipated, it was mainly used by populist parties and foreign powers to infiltrate the ballot-boxes around the globe.

EU elections

Foreign interference in the information domain, often part of a hybrid operation, may be carried out by a foreign state or its agents as part of a coercive and deceptive efforts to disrupt the free information and expression of individuals' democratic choice.[13]
The Commission, the Parliament and the EEAS, closely monitored the foreign information manipulation and interference and disinformation threats before and during the elections and coordinated responses, actively intervening to support a fair electoral space. What had been observed when it came to EU elections was that there was an increase in the volume of information manipulation around the elections, but when it came to the actual elections no large-scale disinformation or manipulation was detected.

According to the European Digital Media Observatory (EDMO) the main disinformation narratives about the EU elections found on social media platforms ranged from:

[11] https://www.euractiv.com/news/draghi-calls-for-deep-cuts-to-privacy-rules-and-pause-on-high-risk-ai-act/
[12] https://theconversation.com/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture-244225
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0790

(a) False stories questioning election integrity.
(b) False narratives alleging the escalation of the war in Ukraine and the direct involvement of EU countries in the conflict.
(c) Recurring false narratives on climate change.
(d) False content portraying migrants as "seizing power" in the EU.[14]

(a)
When it comes to questioning election integrity most instances of disinformation suggested that EU voting procedures were unfair, rigged, manipulated and plagued by invalid ballot boxes. This materialised in reducing voter turnout as disinformation pushed eligible voters to distrusting the electoral process. For example, in **Italy**, false claims circulated regarding how low voter turnout could trigger a withdrawal from the EU. In **Germany**, false stories suggested that voting in the EU elections could be considered a crime or that ballots with holes or corners cut are invalid, when in fact these were put in place to help blind and visually impaired citizens to vote. In **Bulgaria**, social media, websites and traditional media were used to spread disinformation around fake polls.[15]

(b)
False narratives were frequently based on political leaders. In **Ireland** local fact checking units reported in June 2024 that non-white candidates had faced a surge of misinformation and racist abuse. Fringe anti-immigration groups falsely claim these candidates are part of a power grab, also alleging that non-citizens can vote in elections. The Immigrant Council of Ireland reports threats, vandalism, and public confrontations. At the same time, a recurring false story in **Spain** re-emerged claiming that Volt, a registered political party since 2019 is a "fake party" designed to confuse voters or divert votes from Vox, allegedly because its symbol is placed near Vox's one on the ballots. These claims are baseless: Volt, a pan-European party, has participated in multiple elections and the placement of ballots follows an order based on the submission of candidacies.[16]

(c)
In the **Netherlands**, whereby messages on social media falsely alleged how the EU's Green Deal was destroying Europe's food supply.[17] Further disinformation to discredit the EU has been circulating in the Baltic States, claiming falsely that the EU mandated the immediate adoption of electric cars, banning repairs of older vehicles and prohibiting the use of firewood for heating.[18] In **Latvia**, shortly before the elections, another popular myth about the Green Deal made a comeback. It was claimed that due to the EU policies it will be illegal to heat homes using firewood, briquettes and wood pellets. About a year ago, the Latvian Forest Owners' Association spread this myth to pursue its own business interests.[19]

[14] https://disinfocode.eu/structural-indicators/
[15] https://commission.europa.eu/document/download/dd2ddea7-d145-4055-b60c-a32941dc0e84_en?filename=SWD%20-%20Report%20on%20the%202024%20elections%20to%20the%20European%20Parliament.pdf
[16] https://edmo.eu/thematic-areas/elections/european-elections/eu-elections-disinfo-bulletin/#issue43
[17] https://www.euronews.com/green/2024/04/30/conspiracy-theorists-have-turned-from-covid-to-climate-how-will-it-impact-the-eu-elections?utm_source=
[18] https://edmo.eu/publications/old-cars-immigrants-and-war-how-eu-related-misinformation-is-spread-in-the-baltics/
[19] https://edmo.eu/publications/old-cars-immigrants-and-war-how-eu-related-misinformation-is-spread-in-the-baltics/

(d)

Finally, circulated disinformation about migrants seizing power cases were widespread. Once again in **Latvia**, before the election, populist parties also tried to scare the public with stories about migrants. A candidate of the National Alliance, which had become an opposition party after many years in government, said on TikTok that "it looks like Europe will be destroyed not by war, but by another disaster", namely, immigrants. Later, other candidates spread the claim that the recently adopted EU Migration Pact could result in Latvia having to take in 10,000 immigrants or pay 200 million euros a year. This unsubstantiated claim was repeated by the aforementioned party **Latvia First**. This is a similar narrative to **Cyprus's** far-right ELAM party which adhered to the slogan **Cyprus First** in the parliamentary elections of 2021 which also was infringed by disinformation on migration.

USA – Foreign Interference

The US's three main strategic adversaries – **Russia, China and Iran** – were all involved in efforts to influence the 2024 election. This was not their first attempt: Russia interfered in the 2016 election, while China and Iran were active in the 2022 midterms. In 2024, Russia appeared to favour Trump because of the now president-elect's stance on the war in Ukraine and criticism of NATO. Iran, in contrast, was opposed to Trump's return due to his past policy of maximum pressure against Tehran. China did not appear to show a preference for either candidate.[20] In a deeply polarised environment, there was widespread concern that foreign powers could significantly disrupt the election and affect its result in the United States. US agencies had implemented several measures to respond to these malign actions.

Most often the incentive behind foreign interference in local elections has as its motive to undermine electoral integrity and sowing mistrust amongst the electorate, in this case the American electorate.

Groups that were linked to **China**, or at the very least aligned with China operated with the goal of seeding doubt amongst the American voters. Taizi Flood (a.k.a. Spamouflage) had launched campaigns against several Republican politicians who had in the past denounced the People's Republic of China. Roughly two-dozen Taizi Flood accounts posted various narratives accusing Senator Marco Rubio of corruption and connecting him to criticisms made about the Harris-Waltz campaign.[21] During the run-up to the elections similar disinformation emerged from Taizi Flood accounts targeting Republican figures a such as Alabama's Representative Barry Moore, Tennessee Senator Marsha Blackburn and Texas's Representative Michael McCaul.

Taizi Flood utilised various methods such as tagging of prominent politicians and celebrities in their posts and by flagging disinformation that would appeal to the American public such as insider trading, overall corruption, accusations of antisemitic language and abuse of power. The overall messaging of foreign interference looks to undermine the US whilst also depicting its elected officials as untrustworthy.

[20] https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-net-work-focuses-on-us-election/

[21] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-Report-Russia-Iran-and-China-continue-influence-campaigns-in-final-weeks-October-23-2024.pdf

More of the same can be found as **Russian** actors attempted to pivot the Harris-Walz campaign with political deepfakes. In mid-September of 2024, Russian-language accounts on X and Telegram posted an AI-enhanced video of Vice President Kamala Harris falsely depicting her making insensitive references to the assassination attempt against Donald Trump. In the AI-generated audio Harris states the Trump refused to "even die with dignity." Russia has been known of using AI at times, however most Kremlin backed groups employ simple tactics such as deceptive editing and staged videos.[22] There were also Russian backed actors who created a video depicting and framing Harris in an alleged hit and run incident. Furthermore, in October a video emerged on X depicting an individual accusing Governor Tim Walz of sexual assault while a student at Mankato West High School.[23] Russian backed disinformation was targeting Democrat representatives as they seemingly appeared to favour Trump, mostly due to Former President Joe Biden's support of Ukraine.

On a similar note **Iran** too tried to stoke university protests and election abstention for the American backed aid in Israel. The Iranian operated cyber persona called on Americans to boycott U.S. elections and sought to stoke university protests. The group, "Bushnell's Men," which poses as Americans on social media, used Telegram and X (formerly Twitter) to call on Americans to sit out the elections, sending the message that the next U.S. president won't have their support for "aiding Israel in its brutal activities." Bushnell's Men previously sought to stoke anti-Israeli university protests in the United States and Europe in May, in part by remotely printing fliers calling for demonstrations. The group's latest messaging continues to stoke anti-Israeli protests at universities, linking the election boycott to a lack of a ceasefire and claiming that the "Pro-Palestine Student Movement is Still alive"[24]

In the end, the electoral result was not contested. Trump won decisively and efforts made by foreign states to sow uncertainty during the transition period effectively failed. However, much of the credit goes to US authorities, who implemented a well-coordinated counter-interference strategy prior to and on election day. This was a whole-of-government approach, which included non-government agencies as well, and built on the lessons learned from previous elections. It is impossible to know for sure whether these measures would have neutralised the impact of malign activities, especially if the electoral outcome had been less clearcut – for instance, with a more tightly contested electoral college result. Nevertheless, they were key in strengthening the resilience of the electoral process.[25]The EU should also carefully analyse the **US playbook** for 2024. It contains some practices that the EU and Member States already follow, but also some innovative strategies.

[22] https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf
[23] https://www.msn.com/en-us/news/us/fact-check-did-a-former-student-accuse-tim-walz-of-sexual-assault/ar-AA1svHaL?ocid=BingNewsSerp
[24] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-Report-Russia-Iran-and-China-continue-influence-campaigns-in-final-weeks-October-23-2024.pdf
[25] https://www.iss.europa.eu/publications/briefs/future-democracy-lessons-us-fight-against-foreign-electoral-interference-2024

Romania

Over the past eight months, Romania has gone through one of the most turbulent phases of its post-communist democratic history. Following two rounds of presidential elections originally annulled in December 2024 the country ultimately elected pro-European independent candidate Nicușor Dan in May 2025.

The electoral process was heavily influenced by propaganda and disinformation, amplified by Russian interference, which enabled far-right, pro-Russian candidate Călin Georgescu to win the first round, despite having been almost entirely absent from opinion polls only weeks earlier. The unusual circumstances surrounding the presidential race escalated further when Romania's Constitutional Court annulled the 2024 election before the second round concluded, citing "Russian hybrid actions" and the manipulation of TikTok algorithms in Georgescu's favour. This unprecedented ruling divided opinion some viewed it as a long-overdue but necessary intervention, while others denounced it as undemocratic and an abuse of power.[26] The decision pushed Romania into uncharted political and diplomatic territory. In the aftermath, Georgescu, who was elevated to near-messianic status among his supporters, was barred from running in the 2025 election and now faces six charges linked to disinformation, establishing a fascist movement, and undermining the constitutional order.

More specifically, throughout 2024 **more than 34 Russian hybrid attacks against Romania** were documented with **more that 25,000 TikTok accounts and 5,000 Telegram channels** being mobilised in favour of the far-right candidate.[27] Romania, therefore, witnessed ultra-conservative disinformation campaigns against Dan.

One such campaign falsely accused Dan that he did not baptise his children and therefore is not truly an Orthodox Christian, something which would have been a major concern for many Romanian voters given the countries deep conservative Orthodox nature.[28] Additionally a deep-fake video tried to depict the presidential candidate in a synagogue, implying that he was Jewish.[29] Propaganda did not fall only on the pro-western candidate, but it also aimed to portray Russia as the one and only true protector of the Orthodox faith, something that the west was not, according to the Russian campaigns.[30]

However, the annulment of the election in late 2024 was the major tool given to the Russian disinformation campaigners. Widespread criticism of Romanian authorities as well as accusations of a dep-state campaign against Georgescu created a deep notion of paranoia amongst the public. Georgescu's barring from the May 2025 election, along with the annulment of the vote in 2024 were portrayed as proof of democracy itself being cancelled

[26] https://www.friendsofeurope.org/insights/critical-thinking-hybrid-warfare-through-disinformation-the-recent-case-of-romania/
[27] https://stirileprotv.ro/stiri/politic/cum-a-fost-posibil-ca-in-2024-sondajele-de-opinie-sa-nu-l-vada-pe-candidatul-calin-georgescu-explicatia-sefului-inscop.html
[28] https://www.g4media.ro/video-nicusor-dan-lanseaza-doza-de-fake-news-pentru-a-combate-dezinformarile-despre-el-ce-m-a-mahnit-cel-mai-tare-sunt-atacurile-la-familie-nu-credeam-ca-poate-sa-fie-cineva-atat-d.html
[29] https://www.tiktok.com/discover/nicusor-dan-aprinde-flacara-in-sinagoga
[30] https://youtu.be/K6NM3_X_kZ4?si=TzSEFRQJvB9plaRu

in Romania. Some campaigns worked on a platform which spread the idea that the 2025 elections would also be cancelled whilst also hinting that an autocratic regime war forming.[31] Following Dan's win in May a rigged elections narrative was unsurprisingly spread throughout the country, especially in the diaspora of Moldova where Dan had won an 88% majority. The stories circulating were that voters had their votes checked and were blackmailed with losing their jobs.[32]

The Romanian case highlights pressing questions about how best to respond to hybrid threats. Addressing future challenges will require more than simply debunking falsehoods, it will demand strengthening societal resilience through state-led social media education and the use of pre-bunking strategies, initiatives that Romania currently lacks.

France

France too has had a strong share of disinformation with **152 incidents reported between 2023 and 2024** amid the 2024 Olympics and the elections of that year.[33] The French Prime Minister, François Bayrou, stated that after Ukraine, France is the leading European target for foreign disinformation.[34] This is not shocking given the high amount of recorded incidents. Disinformation hit France in early summer 2023 in the build-up to the summer Olympics and included images of blood-stained hands smeared on a Holocaust memorial, coffins placed at the base of the Eiffel Tower and a fabricated French army recruitment campaign urging enlistment for Ukraine.[35]

The online redirection campaigns shifted their focus toward the European elections and continued after President Macron unexpectedly called legislative elections with only three weeks' notice. According to data analysed by *antibot4navalny* and shared with the AP, in the week leading up to the first-round vote on June 30, roughly 75% of posts targeting French audiences either attacked Macron or promoted the far-right National Rally.

One fabricated article, posing as a publication from Le Point and AFP, criticized Macron with the headline: "Our leaders have no idea how ordinary French people live but are ready to destroy France in the name of aid for Ukraine." A fake site masqueraded as Macron's party, offering voters €100 in exchange for their support, while linking back to the party's official website. Yet another fake site inadvertently revealed its own AI-generated methods, leaving behind a prompt instructing a rewrite of an article "taking a conservative stance against the

[31] https://www.stiripesurse.ro/avertisment-din-partea-dianei---osoaca-alegerile-din-mai-pot-fi-anulate-pe-baza-hotararii-curtii-de-apel-ploiesti_3660268.html
[32] https://www.g4media.ro/breaking-george-simion-acuza-o-frauda-la-vot-fara-sa-prezinte-vreo-proba-trebuie-sa-oprim-frauda-imensa-colegii-mei-sunt-cu-conducerea-sts-acum-in-r-moldova-guvernul-a-inceput-sa-fure.html
[33] https://www.lemonde.fr/en/international/article/2025/03/28/disinformation-pm-says-france-is-the-top-eu-target-for-foreign-campaigns_6739602_4.html
[34] https://www.lemonde.fr/en/international/article/2025/03/28/disinformation-pm-says-france-is-the-top-eu-target-for-foreign-campaigns_6739602_4.html
[35] https://apnews.com/article/france-election-disinformation-russia-olympics-be18d688677240686df200096018f221

liberal policies of the Macron administration," according to cybersecurity consultancy Recorded Future's Insikt Group.[36]

France's cybersecurity watchdog, Viginum, has repeatedly flagged Russian disinformation activity, publishing several reports since mid-2023. Around the same time, pro-Kremlin Telegram channels began circulating "Olympics Have Fallen", a fake Netflix-style film using an AI-generated voice mimicking Tom Cruise to criticize the International Olympic Committee.[37]

Disinformation campaigns have thrived on a fragile foundation built over decades of corruption and widespread distrust in institutions, reinforced by repeated failures of governance across the political spectrum. Tackling disinformation alone will not eliminate radicalism; it must be paired with effective governance and regional development that addresses the needs of Romania's, France's, the USA's and in general global long-neglected citizens.

Regulating AI: Legal and Ethical Dilemmas
Resilience: How can we strategically move into the future with the on-going threat of misinformation?

In 2024 a study by the Campaign Legal Centre (CLC) highlighted the danger of political ads that use AI to generate deceptively realistic false content.[38] As seen in the examples of Romania, France and the USA various techniques were used to manipulate voters and mislead the public. Despite the efforts of 20 major tech companies (including Google, Meta, OpenAI and X) to take steps in detection and tracking issues such as deepfakes, most proposed solutions are still a long way from providing tangible protections for voters and instead, leaving them susceptible to manipulations.

The EU has made strong statements on regulating the role of artificial intelligence in our lives. The AI Act has managed to take an active approach which carries significant financial penalties for misuse of AI technology. Yet the issue remains, regulating AI poses an array of challenges.

Challenges

It is well known that since coming into our lives, AI has benefitted society in various sectors, such as in healthcare, transportation, education, and customer services. The challenges however are wide-ranging as we need to ensure that public institutions, legal frameworks and democratic societies uphold essential values such as transparency, accountability and informed consent and decision.

For example, the EU's **AI Act** and its taxonomy of risk issues a transparent way forward whereby any content viewed by users on social media would be organised into levels of risk, thus offering transparency. On the other hand, a key challenge to this is the **lack of AI literacy.** Though legal frameworks and regulation are being practiced in the EU, users might not be

[36] https://apnews.com/article/france-election-disinformation-russia-olympics-be18d688677240686df200096018f221
[37] https://www.france24.com/en/europe/20250507-russia-disinformation-france-ukraine
[38] https://campaignlegal.org/update/how-artificial-intelligence-influences-elections-and-what-we-can-do-about-it

trained to understand what these categorizations mean. Normal questions such as what the difference is between "high-risk" and "limited risk" need to be addressed and easily accessible to users. AI literacy, meaning the skills, knowledge and understanding, is a concept mentioned in the AI Act itself, nonetheless incorporating AI literacy is something that still lags behind the rapid strides that artificial intelligence is making in our lives.

Any AI literacy programmes should aim for trustworthy use of AI, and not just teaching the public how to avoid the penalties and fines included in the 2024 AI Act. This requires an ongoing effort as keeping with AI advancements is itself challenging. Democratic institutions such as the European Parliament should focus on strong campaigns of educating citizens on what the AI Act encompasses and how to spot the various disinformation attempts by foreign agents based on the assigned taxonomy. This would offer a clear path to protection of the public from the darker side of AI and could further safeguard civil society in upcoming elections.

Major challenges remain and the most crucial is that acts surrounding AI should be assessed systematically documented, periodically reviewed and include a roadmap which offers the possibility of abrupt amendment. An AI literacy plan should also promote continuous learning and support this process with appropriate resources, timely information and updated assumptions.[39]

The case of the Spanish Volt - a registered political party since 2019 - illustrates how disinformation can undermine democratic processes. Spanish Volt was falsely labeled as a "fake party" designed to confuse voters into diverting their votes from Vox, mainly because their party symbols appeared similar on the ballot. This confusion could have been prevented if the **AI Act** included a clear and specific category for disinformation within its regulatory framework. Moreover, combining such regulation with improved AI literacy among voters would empower citizens to critically assess and question false narratives, protecting the integrity of elections.[40]

Analogously, in the case of Romania's elections, deepfake videos of presidential candidate Dan in a synagogue should have been properly classed within the AI Act taxonomy and along with local, national and pan-European AI education voters would have been able to identify and ignore such content which is there to disinform the public.
These efforts though challenging should stem from pan-European through MEPs and Political Groups but should also work on national levels and most importantly local levels. By local levels what is meant is that local municipalities should ensure that voters comprehend what the AI Act focuses on and understand the dangers of disinformation.

Is labelling AI-generated content enough?

Labelling AI-generated content can enhance transparency and build trust by helping people identify machine-produced material and make more informed choices about the information they consume, however, is this sufficient enough?

Article 50 of the AI Act, titled "Transparency Obligations for Providers and Deployers of Certain AI Systems," recognizes that certain AI tools especially those that interact with people

[39] https://www.nautadutilh.com/en/insights/ai-literacy-under-the-eu-ai-act-three-key-insights/
[40] https://maldita.es/malditobulo/20240606/papeletas-vox-volt-elecciones/

or generate content pose risks of impersonation or deception even when they are not considered high-risk systems.[41] To address these risks, the Act introduces transparency rules that complement existing high-risk AI regulations. These include informing individuals when they are engaging with AI (unless it is obvious from context) and notifying them if biometric data is analysed to infer emotions, intentions, or categories.[42]

While some provisions of the AI Act have already applied since August 2024, the full implementation date is set for 2 August 2026. This delay has raised concerns, as AI is advancing rapidly and urgent issues like deepfakes and disinformation require immediate attention. To bridge the gap, the EU has launched voluntary initiatives: the Commission's **AI Pact** encourages companies to begin applying the Act's requirements early, while many platforms are independently developing labelling systems to improve transparency and user trust.[43]

As mentioned above, enforcing transparency across global platforms faces major challenges. EU countries have diverse regulatory structures, complicating efforts to create uniform enforcement. Moreover, the AI Act leaves it to Member States to designate supervisory authorities and establish penalties, leading to fragmented oversight. For example, Spain has created a dedicated regulatory body, and Italy has drafted a law on AI, while France and Germany have yet to establish specific frameworks.[44]

Content labelling is an important step toward reducing deception and disinformation, however, it cannot fully address the problem. Sophisticated deepfakes may still bypass detection systems. A stronger response will require a combination of advanced detection tools, tighter regulations, and public education initiatives to raise awareness about deepfake risks and help users recognize manipulated content.

DSA as deterrent?

Additionally, overlaps and tensions with the Digital Services Act (DSA) complicate enforcement. The DSA, in force since February 2024, requires platforms to address liability, appeals, systemic risks, and advertising standards. But generative AI models do not always fit neatly into these categories. For instance, Google's AI Overviews delivers direct answers rather than functioning like a conventional search engine, while private messaging and email services fall outside DSA hosting rules essentially meaning that AI chatbots are also not clearly covered.[45] This forms yet another complication for the AI act when it comes to regulating the darker dimensions of artificial intelligence.

Moving Forward with the AI Act

Article 99 of the AI Act requires Member States to establish rules, enforcement mechanisms, and proportionate penalties for violations, and to notify the Commission of these measures and

[41] https://artificialintelligenceact.eu/article/50/
[42] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
[43] https://digital-strategy.ec.europa.eu/en/policies/ai-pact
[44] https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/
[45] https://www.wired.com/story/google-ai-overviews-how-to-use-how-to-turn-off/

any updates.[46] Failure to comply with the Act's obligations can result in severe fines of up to €35 million or 7 percent of a company's global annual turnover.

While significant financial penalties may act as a deterrent for large organizations, they have limited effectiveness in curbing the creation and spread of deepfakes. Smaller actors, individuals, and entities operating in jurisdictions with weak enforcement are less likely to be restrained by such measures. Moreover, fines only address misconduct after publication, rather than preventing harmful content from being produced or disseminated in the first place. More proactive solutions such as advanced detection technologies and public education are needed to counter deepfakes at an earlier stage.

According to a study by the Columbia Journal of European Law, extraterritorial enforcement poses an additional challenge. The AI Act's scope extends beyond the EU: under Article 2, it applies to providers offering AI systems within the Union, regardless of whether they are based in the EU or abroad. Enforcing penalties against actors outside EU borders, however, is complex and often ineffective. This may require supplementary enforcement tools, including harmonized criminal law frameworks, cooperation with non-EU authorities, and the use of Mutual Legal Assistance Treaties (MLATs).[47]

Addressing the threat of deepfakes therefore calls for a comprehensive strategy. Deploying sophisticated AI-based detection systems on online platforms, paired with real-time monitoring through collaboration between governments and technology companies, can help limit the rapid spread of manipulated content. At the same time, creating an AI literate public is essential: awareness campaigns that build digital literacy and teach citizens how to identify manipulated media can foster critical engagement with online content, reducing the overall influence of disinformation.

The AI Act, along with other regulatory initiatives, can strengthen oversight of AI systems by setting clear standards for their design and use, while also ensuring that AI-driven manipulation is detected earlier.

However, it is uncertain whether financial penalties alone are sufficient to deter violations, especially given the rapid pace of AI innovation. A more effective response requires a combination of advanced detection tools, cooperation between governments, industry, and civil society, and an informed public. These elements are particularly critical in high-stakes contexts such as elections, where deepfakes and other forms of misinformation can distort public opinion and undermine democratic processes.

Ultimately, users play a vital role in defending themselves against deception. By critically assessing the credibility of news, images, and other media, questioning sources, and considering whether content may have been AI-generated, individuals can reduce their vulnerability-at least while AI-generated material remains detectable.

[46] https://artificialintelligenceact.eu/article/99/

[47] https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/

Safeguarding our democracies

As AI adoption grows, legal professionals must ensure safe-guards are in place and balance innovation with public safety. Countries have moved forward in their own ways in order to regulate AI, however how can we move forward with AI regulation in a cohesive legislative manner encompassing a united front from all member states.

National Parliaments role in AI regulation

National parliaments play a crucial role in AI regulation by legislating, overseeing implementation, and supporting innovation through risk-based frameworks and the creation of national bodies. They often initiate **AI-related bills**, align them with supranational frameworks like the EU's AI Act, establish mechanisms for market surveillance and enforcement, and facilitate the development of **regulatory sandboxes** to test and promote innovative AI technologies, ensuring a human-centric approach to AI governance.

In **Austria** a law was passed to establish an AI Service Centre, which has been tasked with analysing AI regulatory frameworks, conducting research and holding expert discussions to both private and public institutions. In **Belgium** a resolution was proposed urging the government to establish policies on workplace AI usage. Furthermore, in December of 2024, a bill was introduced to amend the Code of Criminal Procedure by adding a new article aligned with the EU AI Act. The proposed legislation focuses on the use of AI in the criminal justice system, addressing in particular human rights, public security, criminal procedure and biometrics. Its aim is to ensure compliance with EU regulations while modernizing domestic criminal proceedings.[48] In **Spain** in October 2024, a working group was formed to prepare a comprehensive risk report, including a cybersecurity risk assessment and recommendations for improvement. The Senate's Digital Transformation Committee is reviewing two motions on AI regulation. One of these motions calls for a ban on the misuse of AI in elections, while the second motion calls for measures for the sustainable management of electronic waste from AI and its environmental impact. In January 2024, the **Polish Sejm Committee** for Digitalization, Innovation and Modern Technologies established the Standing Subcommittee on Artificial Intelligence and Algorithm Transparency. The subcommittee has engaged in discussions on the ethical aspects of creating, implementing and using AI systems and has examined EU AI Act in relation to the Polish justice system.

It is evident that European governments have been using legislative means to pass regulations in order to mitigate and regulate the uses of Artificial Intelligence within the political spectrum. Beyond the establishment of specialised committees under governmental auspices, EU member states have been given specialized grants by the European Commission to disseminate amongst university networks, small and medium sized enterprises (SMEs), and centres of excellence for running advanced degree programs in AI. This funding stems as far back as the end of 2020 where the first grants were approved and amounted to a total of 6.5 million euros.[49]

Various bodies therefore have been working on legislation and application of legislative regulation on AI, ranging from AI education to cybersecurity assessments. Main concerns

[48] https://www.lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?legislat=56&dossierID=0601

[49] https://www.europeanpapers.eu/europeanforum/human-centric-perspective-regulation-artificial-intelligence

however surround the privacy and security of data storage and the avoidance of breaches that could compromise sensitive information. **Chat-GPT** is currently widely used in all sectors of personal and professional life. Sensitive information is being shared one way or another, which draws into question fundamentals on human rights. For example, if a medical student uses Chat-GPT in order to prepare patient files this immediately brings into question various legal interrogations, one of which is that of medical confidentiality.

The question here is how can legislative bodies either on a local, national or pan-European level regulate this? In response to this issue, the Italian Data Protection Authority ordered a provisional restriction on the processing of Italian users' data by **Open-AI**. Access was later restored after Open-AI **implemented corrective actions**, including a communication campaign to inform users and options to opt out of data usage.[50] The Italian Data Protection Authority is an independent authority set up to protect fundamental rights and freedoms in connection with the processing of personal data.

In this manner we can delineate how certain legislative and legislative-adjacent bodies are taking up roles on enforcing AI regulations by means of their national parliaments. Action at a European level must be achieved, nonetheless ensuring that national governments apply regulations, either those enlisted within the framework of the AI Act or regulations deemed necessary for specific cases, such as concerns over OpenAI in Italy, are a step forward suggestive of a gradual acceptance of AI's **healthy role** in daily life. Additionally, this demonstrates how local governments are aware of concerns over potential human rights violations and potential hindrance of democratic processes. Regulating at a local level can also benefit wide-ranging AI regulation on European level as it is demonstrative of popular concerns.

The role of European Universities

Europe's uniquely collaborative research system is a strength. Using cooperative approaches creates opportunities to leverage AI, for example through large datasets and many different users. Cooperation should be an integral part of the EU strategy for AI in science. A main concern is that under the risk classification system universities inside the EU should note that they would be considered high-risk AI system providers. This means that universities are required to fulfil a range of obligations.

[50] https://www.biodiritto.org/Online-First-BLJ/Online-First-BLJ-1-22-L-orizzonte-giuridico-dell-Intelligenza-Artificiale

Key requirements:

1. Establish their own risk management system based on that of the AI Act.

2. Conduct data governance - ensuring that training, validation and training datasets are relevant.

3. Draw up technical documentation to demonstrate compliance.

4. Design their high-risk AI system for record-keeping to enable it to automatically record events relevant to identifying national level risks.

5. Design their high-risk AI system to achieve appropriate levels of accuracy, robustness, and cybersecurity.

6. Establish a quality management system to ensure compliance.

Belgian university KU Leuven encourages students, researchers and teaching staff to handle this technology in a responsible and critical way. KU Leuven has formed an expert committee on GenAI in order to internally regulate and monitor.

Their tasks include:

- answering questions from policy, faculties, departments or support services.

- evaluating existing guidelines and information pages and suggesting adjustments according to the latest developments.

- Monitoring that these are sustainable and maintain the necessary flexibility according to the rapidly evolving context.[51]

The **GenAI Expert Committee** guides the university through the developments and challenges of GenAI within the fields of research and education, with an eye on innovation, sustainability and societal relevance. What this suggests is that entities such as universities can pioneer their own path into AI regulation and AI literacy. Universities across Europe have different strategies when handling GenAI, however they ensure as a priority the continuous monitoring of developments on ethical and regulatory standards. Another example is ETH Zurich whereby the university allows its lecturers to explore how GenAI can support their work, nevertheless it assigns responsibility on individual lecturers regarding quality control and checking for possible bias.[52]

[51] https://www.kuleuven.be/english/genai/expert-committee-genai
[52] https://ethz.ch/content/dam/ethz/main/eth-zurich/education/ai_in_education/Generative%20AI%20in%20Teaching%20and%20Learning%20-%20Guidelines%20ETH.pdf

Universities have a dual role in AI regulation: by developing and applying AI, they are regulated entities subject to legal requirements like transparency and data protection, but they also serve as crucial shapers of regulation through ethical research, talent development, global collaboration, and educating the public and future AI professionals on responsible AI use and governance. By creating and implementing internal policies, they build interdisciplinary expert committees and adapt curricula to foster academic integrity and the responsible use of AI technologies, acting as a lighthouse for complex AI challenges.

Similar to the role of national governments, universities have adapted to co-existence with Artificial Intelligence and the need to do so on a regulated path in order to safeguard democratic principles.

Conclusion

Overall, the Artificial Intelligence Act (AI Act) reflects the European Union's strong commitment to safeguarding democratic values, with particular emphasis on media pluralism, freedom of expression, and the protection of civil society from the growing risks of disinformation.

The AI Act adopts a forward-looking perspective, targeting the design, development, and deployment of artificial intelligence systems across the 27 member states. Its focus is not only on mitigating risks related to biased algorithms, surveillance practices, or harmful automation but also on creating a harmonized regulatory framework that fosters innovation while ensuring that AI technologies are safe, fair, and respectful of fundamental rights. Together, these two regulatory initiatives illustrate the EU's dual approach: protecting the integrity of current information ecosystems while preparing for the technological disruptions that AI may bring to future democratic processes.

Nevertheless, significant hindrances and challenges arise in the practical implementation of both Acts. Enforcement will require robust cooperation between regulators, platforms, civil society organizations, and citizens themselves. Moreover, the rapid pace of technological innovation means that legislation alone cannot keep up with every emerging threat. For this reason, the way forward must combine regulation with broader strategies of public education and digital literacy. By empowering citizens to critically assess information, recognize the implications of AI-driven systems, and make informed choices, the EU can foster a resilient society capable of withstanding disinformation campaigns and manipulative practices.

In particular, educating the public on how to navigate the complexities of artificial intelligence, (ranging from algorithmic decision-making to the role of generative models in shaping public discourse), emerges as one of the most viable and sustainable solutions. As Europe looks ahead to future elections, the success of these efforts will depend not only on legal frameworks but also on the cultivation of a digitally literate electorate that can engage with information critically, confidently, and responsibly. With local, national and European efforts, along with strong financial support for these legislations, the move forward toward ensuring that artificial intelligence does not take over these spheres democracy could succeed.

Bibliography

https://www.kuleuven.be/english/genai/expert-committee-genai
https://www.biodiritto.org/Online-First-BLJ/Online-First-BLJ-1-22-L-orizzonte-giuridico-dell-Intelligenza-Artificiale
https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331635
https://www.nytimes.com/2024/04/18/world/asia/india-election-ai.html
https://st.llnl.gov/news/look-back/birth-artificial-intelligence-ai-research?utm_source=chatgpt.com
https://www.historyofdatascience.com/ai-winter-the-highs-and-lows-of-artificial-intelligence/
https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
https://digital-strategy.ec.europa.eu/en/policies/ai-pact
https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#ai-regulation-in-europe-the-first-comprehensive-framework-4
https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#ai-regulation-in-europe-the-first-comprehensive-framework-4
https://www.europarl.europa.eu/topics/en/article/20220422STO27705/the-future-of-ai-the-parliament-s-roadmap-for-the-eu
https://theconversation.com/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture-244225
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0790
https://disinfocode.eu/structural-indicators/
https://commission.europa.eu/document/download/dd2ddea7-d145-4055-b60c-a32941dc0e84_en?filename=SWD%20-%20Report%20on%20the%202024%20elections%20to%20the%20European%20Parliament.pdf
https://edmo.eu/thematic-areas/elections/european-elections/eu-elections-disinfo-bulletin/#issue43
https://www.euronews.com/green/2024/04/30/conspiracy-theorists-have-turned-from-covid-to-climate-how-will-it-impact-the-eu-elections?utm_source=
https://edmo.eu/publications/old-cars-immigrants-and-war-how-eu-related-misinformation-is-spread-in-the-baltics/
https://edmo.eu/publications/old-cars-immigrants-and-war-how-eu-related-misinformation-is-spread-in-the-baltics/
https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-net-work-focuses-on-us-election/
https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-Report-Russia-Iran-and-China-continue-influence-campaigns-in-final-weeks-October-23-2024.pdf
https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf
https://www.msn.com/en-us/news/us/fact-check-did-a-former-student-accuse-tim-walz-of-sexual-assault/ar-AA1svHaL?ocid=BingNewsSerp

https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-Report-Russia-Iran-and-China-continue-influence-campaigns-in-final-weeks-October-23-2024.pdf
https://www.iss.europa.eu/publications/briefs/future-democracy-lessons-us-fight-against-foreign-electoral-interference-2024
https://www.friendsofeurope.org/insights/critical-thinking-hybrid-warfare-through-disinformation-the-recent-case-of-romania/
https://stirileprotv.ro/stiri/politic/cum-a-fost-posibil-ca-in-2024-sondajele-de-opinie-sa-nu-l-vada-pe-candidatul-calin-georgescu-explicatia-sefului-inscop.html
https://www.g4media.ro/video-nicusor-dan-lanseaza-doza-de-fake-news-pentru-a-combate-dezinformarile-despre-el-ce-m-a-mahnit-cel-mai-tare-sunt-atacurile-la-familie-nu-credeam-ca-poate-sa-fie-cineva-atat-d.html
https://www.tiktok.com/discover/nicusor-dan-aprinde-flacara-in-sinagoga
https://youtu.be/K6NM3_X_kZ4?si=TzSEFRQJvB9plaRu
https://www.stiripesurse.ro/avertisment-din-partea-dianei---osoaca-alegerile-din-mai-pot-fi-anulate-pe-baza-hotararii-curtii-de-apel-ploiesti_3660268.html
https://www.g4media.ro/breaking-george-simion-acuza-o-frauda-la-vot-fara-sa-prezinte-vreo-proba-trebuie-sa-oprim-frauda-imensa-colegii-mei-sunt-cu-conducerea-sts-acum-in-r-moldova-guvernul-a-inceput-sa-fure.html
https://www.lemonde.fr/en/international/article/2025/03/28/disinformation-pm-says-france-is-the-top-eu-target-for-foreign-campaigns_6739602_4.html
https://www.lemonde.fr/en/international/article/2025/03/28/disinformation-pm-says-france-is-the-top-eu-target-for-foreign-campaigns_6739602_4.html
https://apnews.com/article/france-election-disinformation-russia-olympics-be18d688677240686df200096018f221
https://apnews.com/article/france-election-disinformation-russia-olympics-be18d688677240686df200096018f221
https://www.france24.com/en/europe/20250507-russia-disinformation-france-ukraine
https://campaignlegal.org/update/how-artificial-intelligence-influences-elections-and-what-we-can-do-about-it
https://www.nautadutilh.com/en/insights/ai-literacy-under-the-eu-ai-act-three-key-insights/
https://maldita.es/malditobulo/20240606/papeletas-vox-volt-elecciones/
https://artificialintelligenceact.eu/article/50/
https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
https://digital-strategy.ec.europa.eu/en/policies/ai-pact
https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/
https://www.wired.com/story/google-ai-overviews-how-to-use-how-to-turn-off/
https://artificialintelligenceact.eu/article/99/
https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/
https://www.lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?legislat=56&dossierID=0601
https://www.europeanpapers.eu/europeanforum/human-centric-perspective-regulation-artificial-intelligence

https://ethz.ch/content/dam/ethz/main/eth-zurich/education/ai_in_education/Generative%20AI%20in%20Teaching%20and%20Learning%20-%20Guidelines%20ETH.pdf

Appendix

EU Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
EU Artificial Intelligence Pact : https://digital-strategy.ec.europa.eu/en/node/12158/printable/pdf
Digital Services Act Package : https://digital-strategy.ec.europa.eu/en/node/27/printable/pdf