



ITSS
International Team
For the Study of Security
Verona

**Generative AI, Disinformation, and Electoral Integrity:
The EU's Response to Democratic Challenges**

by Antonella Benedetto

ITSS Verona Magazine, Vol. 4, n. 1

Spring/Summer 2025

Generative AI, Disinformation, and Electoral Integrity: The EU's Response to Democratic Challenges

Antonella Benedetto

To cite this article: Antonella Benedetto, *Generative AI, Disinformation, and Electoral Integrity: The EU's Response to Democratic Challenges*, ITSS Verona Magazine, Vol. 4, no. 1, Spring/Summer 2025.

Keywords: Artificial Intelligence, Generative AI, Disinformation, Elections, Democracy, European Union

ITSS Verona website: <https://www.itssverona.it/itss-magazine>

LinkedIn: <https://www.linkedin.com/company/itss-verona/>

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Published online: September 22nd, 2025

Abstract: This article examines the implications of artificial intelligence (AI) in political campaigns, the ethical challenges, and the legal measures being adopted by the European Union (EU) to ensure election transparency and prevent manipulation. All over the world, the rapid advancement of Generative AI (GenAI), particularly through large language models (LLMs) like ChatGPT, Gemini, and DeepSeek, is transforming numerous fields, including human-AI collaboration, content creation, and human-computer interaction. While these technologies enhance human capabilities, they also raise significant concerns, particularly in political campaigns and elections. The primary issues involve potential political biases, misinformation, privacy violations, and the use of deep fakes. LLMs, trained on vast amounts of data, can produce human-like responses and have applications ranging from chatbots to content creation. However, their biases, particularly in political orientations and demographics, can distort the information they generate. Furthermore, the ability of AI to create highly convincing disinformation, such as deep fakes, threatens to undermine democratic processes. AI technologies are increasingly being used in political campaigns for voter targeting, personalised messaging, and strategy optimisation, which improves engagement but also opens the door to manipulation. Recent elections have already witnessed the use of AI-generated content to deceive voters and influence outcomes. In response, the European Union has implemented several regulatory measures, including the Code of Practice of Disinformation, Digital Services Act (DSA) and the AI Act, to combat AI-generated disinformation and safeguard electoral integrity.¹

¹ The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

This article explores how AI technologies are being used in electoral processes, the risks they pose, and the measures the European Union (EU) is implementing to safeguard democratic legitimacy in a digital age. The digital transformation of politics has taken a significant turn with the rise of Generative Artificial Intelligence (GenAI), particularly through Large Language Models (LLM) such as ChatGPT, Gemini, and DeepSeek. While GenAI offers unprecedented opportunities for enhancing campaign strategy, voter outreach, and civil participation, it also introduces serious threats to electoral integrity, including misinformation, deep fakes, and the manipulation of public opinion.

Democratic elections around the world took place in 2024 and 2025. From personalised disinformation campaigns in India to deep fakes in Germany and the United States, the GenAI content poses a direct challenge to truth-based political discourse. Against this, the EU is emerging as a global frontrunner in responding to the democratic risks posed by GenAI. Through legislation like the Digital Services Act (DSA) and the recently adopted and currently implemented AI Act (AIA), the EU is seeking to establish a robust legal and ethical framework that ensures transparency, accountability, and the protection of fundamental human rights.

Generative AI and Large Language Models: Definitions and Impact

Generative AI (GenAI) is transforming fields such as human-AI collaboration, content creation, and human-computer interaction, enhancing human skills in unprecedented ways. Nevertheless, the use of GenAI and of the large language models (LLMs) like ChatGPT, Gemini and the most recent DeepSeek has prompted concerns about potential political biases and their impact on information dissemination and online election interference, even disrupting democratic processes.² LLMs are a subset of AI trained on massive volumes of data. They exhibit human-like responses and understand normal language. These models use

² Emilio Ferrara, "Charting the Landscape of Nefarious Uses of Generative Artificial Intelligence for Online Election Interference," *SSRN Electronic Journal* (2024): 2. <https://doi.org/10.2139/ssrn.4614223>.

advanced machine learning (ML) techniques to analyse and comprehend human speech, including syntax, semantics, and context. Applications for them include chatbots, virtual assistants, content creation, language translation, and scientific research.³ LLMs have even replaced traditional search engines like Google Search, expanding their utility in personal information searches. Nevertheless, the use of AI in political campaigns and elections raises serious ethical concerns. Firstly, the production of inaccurate information and biases. LLMs profess to be neutral and objective during training, yet evidence shows bias in political orientation, gender, colour, and religion.⁴ Secondly, AI may threaten the privacy and security of personal data, as its collection and analysis could infringe upon voters' privacy rights. Third, the spread of misinformation and fake news on social media also constitute a further risk, with a possible consequence to undermine the democratic process. Finally, the spreading impact of deep fakes, that is the creation of realistic fake videos or audio recordings. Deepfakes can be used to misrepresent political candidates or modify their words, causing public confusion and distrust.⁵

Employment of GenAI in political campaigns: benefits and risks

Political campaigns are using AI for three main goals: data analysis and voter targeting, personalised messaging, and strategy optimisation. Regarding data analysis, AI systems can uncover patterns and trends that human analysts may overlook, identifying crucial voter segments who are more likely to be influenced by specific messaging. Precision in voter targeting allows campaigns to distribute resources more efficiently, focusing on those

³ George-Cristinel Rotaru, Sorin Anagnoste, and Vasile-Marian Oancea, "How Artificial Intelligence Can Influence Elections: Analyzing the Large Language Models (LLMs) Political Bias," *Proceedings of the International Conference on Business Excellence* 18, no. 1 (June 1, 2024): 1. <https://doi.org/10.2478/picbe-2024-0158>.

⁴ Yejin Bang, Delong Chen, Nayeon Lee, and Pascale Fung, "Measuring Political Bias in Large Language Models: What Is Said and How It Is Said," in *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)* (Bangkok, Thailand: Association for Computational Linguistics, 2024): 11142. <https://aclanthology.org/2024.acl-long.600>.

⁵ M.B.E. Islam, M. Haseeb, H. Batool, N. Ahtasham, and Z. Muhammad, "AI Threats to Politics, Elections, and Democracy: A Blockchain-Based Deepfake Authenticity Verification Framework," *Blockchains* 2, no. 4 (2024): 459. <https://doi.org/10.3390/blockchains2040020>.

who need it the most likely to be influenced. About personalised messaging, AI enables the creation of tailored messages that align with individual voters' preferences, concerns, and behaviours. This hyper-personalisation improves the effectiveness of campaign communications by making messages more likely to engage voters when they feel directly addressed and understood. Finally, the use of AI in strategy optimisation allows for continuous adaptation based on projected outcomes, leading to more proactive and impactful initiatives. This applies to advertising, public appearances, and policy announcements.⁶ Nevertheless, these developments present new ethical challenges, particularly in terms of privacy and manipulation that will be analysed later on.

The use of AI in political campaigns has led to unprecedented benefits and efficiencies:

- Effectiveness and enhancement in voters' engagement: personalisation can strengthen the relationship between politicians and voters, potentially improving turnout and engagement in the political process. Chatbots may provide 24/7 support for voters, while algorithms optimise email and social media marketing for optimum interaction.
- Better resource allocation: AI can optimise the use of resources by evaluating patterns and forecasting voter behaviour to reach target demographics efficiently.
- Real-time responsiveness: AI systems can analyse real-time data from various sources, such as social media, news outlets, and campaign analytics, to provide insights into public opinion and campaign effectiveness.
- Optimised targeting audience: using data analysis and machine learning, campaigns may tailor their messages to each voter demographic, ensuring relevance and proper delivery channels.

⁶ Yu, Chen. "How Will AI Steal Our Elections?" *OSF Preprints* (un7ev). Center for Open Science, (2024): 2. <https://osf.io/un7ev>.

Advancements in technology offer a promising future for the political process, allowing campaigns to engage with voters more effectively. While AI has many positives, it is important to avoid its misuse and ensure that its use in political campaigns enhances, rather than undermines, election integrity by preventing the spread of misinformation, the manipulation of voters' opinions, and the amplification of divisive content. These possibilities are realistic since AI can generate convincing fake news, deep fakes, and other forms of disinformation. In January 2024, voters in New Hampshire received phone calls that mimicked President Joe Biden's voice, advising them not to vote in the primary election. These calls were identified as AI-generated.⁷ Another important element to consider is the speed at which contents are being created. AI-generated disinformation has the potential to spread quickly and widely: it can quickly manufacture disinformation, leading to a torrent of falsehoods that can disrupt public discourse, making it difficult for individuals, platforms, and agencies to detect and mitigate them. Beyond time, the sophisticated quality of AI technologies and the adaptability of malicious actors made it increasingly difficult to distinguish from genuine content.⁸

Actual risks and documented cases from Asia, Europe and the US

The risks associated with the use of AI in political campaigns are not merely theoretical, they have already materialised in recent electoral processes across the globe. The year 2024 saw democratic elections in more than 60 countries, representing half of the global population and involving 4 billion voters for presidential, legislative, regional and local elections.⁹ The parliamentary elections held in Bangladesh (January 7, 2024) and Pakistan

⁷ Harry Yaojun Yan et al., "The Origin of Public Concerns over AI Supercharging Misinformation in the 2024 U.S. Presidential Election," *Harvard Kennedy School Misinformation Review*, January 30 (2025): 2. <https://doi.org/10.37016/mr-2020-171>.

⁸ Wiederhold, Brenda K. "Unmasking Deception: Strategies to Combat AI-Driven Disinformation." *Cyberpsychology, Behavior, and Social Networking* 27, no. 11 (2024): 747. <https://doi.org/10.1089/cyber.2024.0467>.

⁹ Aditya Kumar Shukla and Shraddha Tripathi, "AI-Generated Misinformation in the Election Year 2024: Measures of European Union," *Frontiers in Political Science* 6 (2024): 2. <https://doi.org/10.3389/fpos.2024.1451601>.

(February 8, 2024) sparked concerns about AI-generated material and potential compromises in the electoral process. Indonesia's elections on February 14, 2024, were likewise challenged by deep fakes. Indian elections in May-June 2024 also posed different misinformation challenges: AI-edited videos circulated among Indian voters, alleging that the ruling party would remove reservations and modify the constitution if elected again.¹⁰

These challenges are not only confined to Asia. In Europe, similar concerns have emerged. In the lead up to Germany's February 23, 2024 election, far-right actors reportedly leveraged AI tools to win. The video of the ultraconservative candidate Alice Weidel started with a question: "Do you remember how beautiful Germany once was?" The video showed a country that never existed: indeed, it was created by AI. AI-generated content like this is assisting Weidel's anti-migration, populist Alternative for Germany (AfD) party by making both parts of its message feel very real — the hopeful, nostalgic future it promises and the scary future it warns could happen if others win the election.¹¹

Another example comes from the United States. At the end of February, a musical video titled "Trump Gaza", generated by AI, was published on *Truth*, US president Donald Trump's social media platform. The video begins by showing the conditions of the Strip-after fifteen months of Israeli bombings and 48,000 confirmed Palestinian deaths – then depicts what is supposed to be the "Gaza Riviera" promised by Trump. In the clip, the present is a 2025 of rubble, soldiers with Kalashnikovs and crying children. After a brief interlude of construction sites, the presidential "What's next" vision finally appears: a waterfront ending in a re-creation of a skyscraper, a main street of markets and palm trees where children finally run to play with balloons shaped like Trump's big face. A statue eventually relaxes with a drink by the pool in the company of Israeli Prime Minister Benjamin Netanyahu, while Elon

¹⁰ See note above.

¹¹ Emily Schultheis, "How Germany's Far Right Is Harnessing AI to Win Votes," *Politico*, February 20, 2025, <https://www.politico.eu/article/germany-far-right-harness-artificial-intelligence-win-election/>.

Musk enjoys a plate of hummus.¹² These examples evidence the profound influence that AI-Generated disinformation, including deep fakes, can have on shaping public perception and manipulating political narratives. This poses a serious challenge for democratic societies: when voters can no longer distinguish the truth, the foundation of informed electoral choice might erode. Moreover, such content is often tailored to exploit emotional reactions - fear, nostalgia, or hope - making it more likely to go viral and bypass rational scrutiny. Due to the rapidity and scale at which these threats occur, regulating and responding to them remains a significant challenge. Nevertheless, unlike other global actors such as the United States — where regulatory responses to AI-generated disinformation remain fragmented or largely self-regulatory — the European Union has taken concrete legislative steps. The Digital Services Act (DSA) and, more recently, the AI Act (AIA) represent an essential effort by the EU to safeguard electoral integrity and democratic process in the digital environment.

EU Study and measures: the Digital Services Act (DSA) and the AI Act (AIA)

The European Digital Media Observatory (EDMO) Task Force on 2024 European Parliament Elections published a study on disinformation. The analysis examined 900 fact-checking articles published throughout 11 elections across 10 European states until October 2023. The report uncovered widespread deception regarding the political process, including false claims of voter fraud, foreign meddling, and unfair tactics.¹³ Despite projections that by 2026, ninety percent of the online content will be generated synthetically,¹⁴ countries and international organisations struggle to regulate AI, primarily because a shared

¹² Francesco Prisco, “How Trump Used AI to Reimagine Gaza as a Luxury Riviera,” *Il Sole 24 Ore*, February 26, 2025, <https://www.ilssole24ore.com/art/trump-posta-video-riviera-gaza-grattacieli-e-danzatrici-AGB6u89C>.

¹³ European Digital Media Observatory (EDMO) Task Force on 2024 European Parliament Elections, *Disinformation Narratives During the 2023 Elections in Europe*, November 2023, <https://edmo.eu/wp-content/uploads/2023/10/EDMO-TF-Elections-disinformation-narratives-2023.pdf>.

¹⁴ European Parliamentary Research Service (EPRS), *AI and Disinformation: How Artificial Intelligence is Reshaping the Disinformation Landscape*. Brussels: European Parliament, 2023, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI\(2023\)751478_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf).

definition does not yet exist.¹⁵ Ahead of European June 2024 elections, the EU took preventative measures to combat false information and AI-generated deep fakes, using a multifaceted approach to address the issue. To mention a few, the *Digital Services Act* requires internet companies like Facebook and TikTok to identify and label modified audio and imagery, including deep fakes to promote transparency and user awareness.¹⁶ In February 2025, the Commission released an elections toolkit that provides practical guidance on how to use the *Digital Services Act (DSA) Election Guidelines* throughout electoral procedures. The toolkit provides best practices and recommendations in four critical areas: stakeholder management, communication and media literacy, incident response, and monitoring and analysis of election-related risks. By offering this guidance, the toolkit supports the Commission's and Member States' continuous efforts to protect the integrity of EU electoral procedures.¹⁷ Another important instrument is the AI Act (AIA), which entered into force in August 2024: it aims to establish a complete legal framework to reduce the hazards of deep fakes. The AI Act can be applied horizontally and provides a risk-based approach: unacceptable risk, high risk, limited risk, and minimal risk.¹⁸

- Unacceptable risk: AI systems that pose a threat to fundamental human rights should be prohibited. As of February 2, 2025, the Commission has banned such harmful systems, to mention a few: manipulation and deception, social scoring, individual criminal offence risk assessment or prediction, practices with the final goal to expand

¹⁵ P. M. Krafft, Meg Young, Michael Katell, Karen Huang, and Ghislain Bugingo, "Defining AI in Policy versus Practice," *arXiv* (2019): 2. <https://arxiv.org/abs/1912.11095>.

¹⁶ European Council of the European Union, *EU Introduces New Rules on Transparency and Targeting of Political Advertising*. Brussels, March 11, 2024, <https://www.consilium.europa.eu/en/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising>.

¹⁷ European Commission, *DSA Elections Toolkit for Digital Services Coordinators*. Brussels, February 2025, <https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators>.

¹⁸ European Commission, *Regulatory Framework for AI*. Digital Strategy, European Commission, 2025. Accessed March 30, 2025, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

the facial recognition databases, emotion recognition in public places, biometric categorisation, and real-time remote biometric identification.¹⁹

- High risk: AI technologies which pose serious risk to health, safety or fundamental rights (safety components in critical infrastructures, CV and exam scorings, safety components, border control management, justice administration) will undergo thorough strict obligation before their commercial release.
- Limited risk: the AI Act establishes clear disclosure requirements to maintain trust by ensuring that individuals are informed when necessary. For example, when interacting with AI systems like chatbots, users should be notified that they are communicating with a machine, enabling them to make informed decisions.²⁰ Deepfakes fall into this category. The AIA does not ban deepfakes completely but imposes strict transparency requirements on both providers and users.²¹
- Minimal risk: the AI Act does not establish regulations for AI systems that are considered to pose minimal or no risk. Most AI systems currently in use within the EU fall into this category, including applications such as AI-powered video games and spam filters.²²

Article 60 (Chapter VI) of the AIA provides a definition of ‘deep fake’ as “AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.”²³ The inclusion of the word “objects” in the legal definition allows it to expand beyond persons, places, events, encompassing any tangible or intangible item that could

¹⁹ See note above.

²⁰ See note above.

²¹ Gernot Fritz, Theresa Ehlen, and Tina Fokter Cuvan, “EU AI Act Unpacked: 8 New Rules on Deepfakes,” web log, *Freshfields* (blog), June 26, 2024, <https://technologyquotient.freshfields.com/post/102jb19/eu-ai-act-unpacked-8-new-rules-on-deepfakes>.

²² See note 18.

²³ European Parliament and Council of the European Union, *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 15 July 2024 on Artificial Intelligence*. Brussels: EUR-Lex, 2024. Accessed March 30, 2025, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>.

misrepresent or alter reality. Also, the inclusion of the term “entities” permits to include businesses, government and NGOs.²⁴

The inclusion of broad terms such as “objects” and “entities” in Article 60 of the AI Act brings notable advantages in media regulation. This broad scope allows the legislation to respond not only to the impersonation of individuals, but also to the falsification of symbols, institutional communications, and other elements that can distort public understanding. As Łabuz argues, this comprehensive framing helps unify fragmented regulatory approaches across different domains, such as disinformation, fraud, and reputational harm, offering a more coherent legal framework²⁵. Meding and Sorge also highlight that this inclusivity enables regulators to better distinguish between benign forms of AI-generated content and manipulative deep fakes intended to deceive, above all in the context of political campaigns, where visual authenticity and institutional credibility are central to public trust. The proliferation of AI-generated disinformation during elections can mislead voters, suppress turnout, or unfairly damage political opponents - outcomes that the AIA attempts to mitigate through clear definitions and transparency obligations²⁶.

While the AI Act’s inclusion of “objects” and “entities” in the definition of deep fakes represents a significant step beyond traditional legislation, it also introduces interpretative challenges. The broad scope may create some ambiguity for developers and deployers in distinguishing between harmful manipulation and more acceptable forms of content editing. Similarly, while the transparency obligations represent a crucial step toward ensuring accountability and building public trust, their practical implementation may require further guidance to ensure clarity and effectiveness. Importantly, the Act rightly emphasises that

²⁴ See note 21.

²⁵ Mateusz Łabuz, “Deep Fakes and the Artificial Intelligence Act—An Important Signal or a Missed Opportunity?” *Policy & Internet* 16 (2024): 783. <https://doi.org/10.1002/poi3.406>.

²⁶ Kristof Meding and Christoph Sorge, “What constitutes a Deep Fake? The blurry line between legitimate processing and manipulation under the EU AI Act”, *Proceedings of the 2025 Symposium on Computer Science and Law (CSLAW '25)*. Association for Computing Machinery, New York, NY, USA (2025): 152. <https://doi.org/10.1145/3709025.3712218>.

transparency requirements should not undermine fundamental rights such as freedom of expression and artistic freedom—though careful implementation will be key to preserving this balance.²⁷

The EU also encourages major digital companies to create tools for detecting and deleting deepfakes from their platforms, particularly during crucial events like elections. TikTok and Meta established fact-checking hubs and “election centres” for the 2024 EU elections. Moreover, article 4 of the AI Act encourages literacy on the topic, calling for investment in public awareness programs to educate citizens on spotting deep fakes and becoming critical consumers of internet content. This includes fostering media literacy and fact-checking methods.²⁸

To curb the harmful impact of AI, some tools can be developed. The private sector often adopts the watermarking technique to detect AI-generated material by adding a visual label. Unfortunately, existing AI watermarking solutions are unreliable and easily circumvented. For example, in January 2023, OpenAI released an AI text detector for ChatGPT built by Aaronson and other academics. Six months later, because of the low accuracy rate, OpenAI removed the AI classifier tool.²⁹ Moreover, the EU legal framework works as a shield against the risks connected to the improper use of AI tools. For example, the General Data Protection Regulation (EU) 2016/679 (GDPR) and EU Data Protection Regulation (EU) 2018/1725 provide users with the ability to object to profiling, as well as restrictions on sensitive personal data use. In 2022, after a long period of negotiation, the Commission adopted the Code of Practice on Disinformation. The industry promised to improve transparency in political advertising by providing more efficient labelling, revealing the sponsor, advertising budget, and display period. The Code intends to empower users by

²⁷ See note 26.

²⁸ See note 9.

²⁹ Lev Craig, “What Is AI Watermarking and How Does It Work?,” web log, *Search Enterprise AI* (blog), October 31, 2023, <https://www.techtarget.com/searchenterpriseai/definition/AI-watermarking>.

providing tools for identifying and flagging deception, accessing reliable sources, and promoting media literacy.³⁰ One of the most important instruments adopted by the EU is the Digital Service Act (DSA). Entered into force in November 2022, it provides a risk-based approach for online platforms to prevent abuse – such as disinformation and mitigating possible harmful content on their platform. In March 2024, the Council approved a new Regulation ((EU) 2024/900) on the openness and targeting of political advertising, aimed at combating information manipulation and foreign intervention in elections. The Regulation stresses three main points: political advertisements must have a transparency label and an easy-to-find transparency notice; online political advertising will only be permitted under tight restrictions; to prevent foreign meddling, advertising services for third-country sponsors will be prohibited three months before an election or referendum. Last but not least, in February 2025, the Commission presented a new best-practice election toolkit on the Digital Service Act to be applied during the electoral processes.³¹

Conclusion

The integration of AI – especially Generative AI and Large Language Models (LLM) – into political campaigns is a double-edged sword. On one side, it offers unprecedented opportunities to enhance voters' engagement, personalise communication, and optimise campaign strategies. On the other hand, it poses profound ethical and legal challenges, ranging from data privacy violations and algorithmic bias, misinformation and the manipulation of public opinion through deep fakes. As societies increasingly rely on digital tools, the risk of AI-driven interference on electoral processes becomes more urgent. The EU's regulatory response, including the Digital Services Act and the AI Act, reflects a proactive approach to safeguard democratic integrity. By establishing risk classification, rules

³⁰ European Commission, *2018 Code of Practice on Disinformation*. Brussels: European Commission, 2018, <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation>.

³¹ See note 16.

for transparency and accountability, the EU has taken a decisive step toward mitigating the misuse of AI in the political context.

Bibliography

- Bang, Yejin, Delong Chen, Nayeon Lee, and Pascale Fung. “Measuring Political Bias in Large Language Models: What Is Said and How It Is Said.” *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (2024)*, 11142–59. <https://aclanthology.org/2024.acl-long.600/>.
- Craig, Lev. 2023. “What Is AI Watermarking and How Does It Work?” *Search Enterprise AI*, October 31. <https://www.techtarget.com/searchenterpriseai/definition/AI-watermarking>.
- Columbia Journal of European Law*, “Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Generated Misinformation,” *Columbia Journal of European Law* (blog), 2024, <https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/>.
- European Council of the European Union. *EU Introduces New Rules on Transparency and Targeting of Political Advertising*. Brussels: European Council of the European Union, March 11, 2024. <https://www.consilium.europa.eu/en/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising>.
- European Commission. *2018 Code of Practice on Disinformation*. Brussels: European Commission, 2018. <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation>.
- European Commission. *DSA Elections Toolkit for Digital Services Coordinators*. Brussels: European Commission, February 2025. <https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators>.
- European Commission. *Regulatory Framework for AI*. Digital Strategy, European Commission, 2025. Accessed March 30, 2025. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.
- European Digital Media Observatory (EDMO) Task Force on 2024 European Parliament Elections. Publication. *Disinformation Narratives during the 2023 Elections in Europe*, November 2023. <https://edmo.eu/wp-content/uploads/2023/10/EDMO-TF-Elections-disinformation-narratives-2023.pdf>.

- European Parliament and Council of the European Union. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 15 July 2024 on Artificial Intelligence*. Brussels: EUR-Lex, 2024. Accessed March 30, 2025.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>.
- European Parliamentary Research Service (EPRS). *AI and Disinformation: How Artificial Intelligence is Reshaping the Disinformation Landscape*. Brussels: European Parliament, 2023.
[https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI\(2023\)751478_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf).
- Ferrara, Emilio. “Charting the Landscape of Nefarious Uses of Generative Artificial Intelligence for Online Election Interference.” *SSRN Electronic Journal*, 2024, 1-16.
<https://ssrn.com/abstract=4883403>.
- Fritz, Gernot, Theresa Ehlen, and Tina Fokter Cuvan. “EU AI Act Unpacked: 8 New Rules on Deepfakes.” Web log. *Freshfields* (blog), June 26, 2024.
<https://technologyquotient.freshfields.com/post/102jb19/eu-ai-act-unpacked-8-new-rules-on-deepfakes>.
- Gernot Fritz, Theresa Ehlen, and Tina Fokter Cuvan, “EU AI Act Unpacked: 8 New Rules on Deepfakes,” web log, *Freshfields* (blog), June 26, 2024,
<https://technologyquotient.freshfields.com/post/102jb19/eu-ai-act-unpacked-8-new-rules-on-deepfakes>.
- Krafft, P. M., Young, M., Katell, M., Huang, K., and Bugingo, G. 2020. "Defining AI in Policy versus Practice." *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, February, 72–78.
- Kristof Meding and Christoph Sorge. 2025. What constitutes a Deep Fake? The blurry line between legitimate processing and manipulation under the EU AI Act. In *Proceedings of the 2025 Symposium on Computer Science and Law (CSLAW '25)*. Association for Computing Machinery, New York, NY, USA, 152–159.
<https://doi.org/10.1145/3709025.3712218>.
- M. Łabuz, “Deep Fakes and the Artificial Intelligence Act—An Important Signal or a Missed Opportunity?” *Policy & Internet* 16 (2024): 783–800,
<https://doi.org/10.1002/poi3.406>.
- Masabah Bint E. Islam, Muhammad Haseeb, Hina Batool, Nasir Ahtasham and Zia Muhammad, “AI Threats to Politics, Elections, and Democracy: A Blockchain-Based Deepfake Authenticity Verification Framework.” *Blockchains* 2, no. 4 (2024): 458–81.
<https://doi.org/10.3390/blockchains2040020>.

- Rotaru, George-Cristinel, Sorin Anagnoste, and Vasile-Marian Oancea. "How Artificial Intelligence Can Influence Elections: Analyzing the Large Language Models (LLMs) Political Bias." *Proceedings of the International Conference on Business Excellence* 18, no. 1 (2024): 1882–91. <https://doi.org/10.2478/picbe-2024-0158>.
- Prisco, Francesco. "Trump posta video 'Riviera Gaza' con grattacieli e danzatrici." *Il Sole 24 Ore*, February 26, 2025. <https://www.ilssole24ore.com/art/trump-posta-video-riviera-gaza-grattacieli-e-danzatrici-AGB6u89C>.
- Schultheis, Emily. "How Germany's Far Right Is Harnessing AI to Win Votes." *Politico*, February 20, 2025. <https://www.politico.eu/article/germany-far-right-harness-artificial-intelligence-win-election/>.
- Shukla, Aditya Kumar, and Shraddha Tripathi. "AI-Generated Misinformation in the Election Year 2024: Measures of European Union." *Frontiers in Political Science* 6 (2024): 1451601, 1-4. <https://doi.org/10.3389/fpos.2024.1451601>.
- Yan, Harry Yaojun, Garrett Morrow, Kai-Cheng Yang, and John Wihbey. "The Origin of Public Concerns over AI Supercharging Misinformation in the 2024 U.S. Presidential Election." *Harvard Kennedy School Misinformation Review*, January 30, 2025, 1-13. <https://doi.org/10.37016/mr-2020-171>.
- Yu, Chen. 2024. "How Will AI Steal Our Elections?" *OSF Preprints* (un7ev). Center for Open Science, 1-24. <https://osf.io/un7ev>.
- Wiederhold, Brenda K. "Unmasking Deception: Strategies to Combat AI-Driven Disinformation." *Cyberpsychology, Behavior, and Social Networking* 27, no. 11 (2024): 747–49. <https://doi.org/10.1089/cyber.2024.0045>.