

# AIDA Working Paper on 'Al and the Future of Democracy'

following the AIDA/INGE public hearing on 15 April 2021



#### Introduction



At the AIDA Committee meeting of 15 April 2021, in cooperation with the Special Committee on Foreign Interference in all Democratic Processes in the European Union including Disinformation (INGE), AIDA and INGE Members heard two panel discussions on the topics of AI and the future of democracy, and on tech developments and regulatory approaches to disinformation. The key takeaways from both panels are summarised below, followed by contributions on the outcome of the hearing made by the European Parliament political groups. A recording of the event is available via the AIDA Committee website<sup>1</sup>.

To guide Members and panellists through the hearing, the following questions were raised to frame the debate: What impact is Al having on democratic and electoral processes? How is Al affecting the notions of active citizenship and political participation? What effects will Al have on democratic institutions and policy-making? These issues were identified as being at the forefront of the challenges the EU is facing in its current trajectory of regulating Al and other emerging technologies, as well as responding to ever increasing volumes of misinformation and disinformation on social media.

In December 2020, the <u>European Commission published the European Democracy Action Plan<sup>2</sup></u>, with the goal of building more resilient democracies across the EU by focusing on three pillars of regulatory and

legislative action: promoting free and fair elections, strengthening media freedom and pluralism, and countering disinformation. In addition, the <u>Digital Services Act package</u><sup>3</sup> was adopted by the Commission as part of the European Digital Strategy, 'Shaping Europe's Digital Future'.

Against this background, the rapid uptake of Al by both public and private actors coupled with the ever-increasing availability of data raises a host of questions for the future evolution of democracies within and beyond the EU. From sentiment analysis to deep fakes, Al technologies can be used to both further and disrupt democratic participation and accountability, while also potentially amplifying trends of polarisation and growing authoritarianism.

To counter these trends, more cooperation is needed at international level, especially between the EU and the US. The newly proposed transatlantic agenda for global change<sup>4</sup> adopted by the European Commission features the establishment of a Transatlantic AI Agreement<sup>5</sup> and an EU-US Trade and Technology Council<sup>6</sup>. Across the Atlantic, the Biden Administration has announced a future Summit of Democracies aimed at "renewing the spirit and shared purpose of the nations of the Free World" <sup>7</sup>. The goal of the summit will be for participating countries to issue a call to action for the private sector, focusing on large social media platforms and technology companies, urging them to



make concrete pledges for ensuring the preservation of democratic societies and protection of free speech. By collectively adopting technologies which safeguard fair electoral processes and combat new forms of disinformation, countries which share the same values can advance towards forming a technological alliance of democracies<sup>8</sup>.

Opening the hearing, **AIDA Chair Dragoş Tudorache** stated: "At the dawn of the digital age, we must set in place rules, worldwide, which will ensure AI will not be used to undermine democracy. First, we need to look inward, and ensure that we do not allow the use of AI for undemocratic practices such as mass surveillance, mass social scoring by the state, or discrimination in Europe. Second, we must reach out to the

world's democracies and work together to build an alliance of digital democracies strong enough to set the rules, standards, and red lines of a democratic digital future, worldwide. Third, we need to ensure that we are protected -- by strengthening our cybersecurity, increasing our own citizens' resilience to fake news and disinformation through education, and developing cutting-edge tools to counter cutting-edge attacks. Last but not least, we need to understand that Al-powered attacks on democracy can be even more devastating than conventional attacks and we must treat them as such. This needs to be reflected in our defence policy, in our cooperation with and participation in NATO, in our transatlantic alliance, and in our global strategy."

- 1 AIDA website, <a href="https://www.europarl.europa.eu/committees/en/aida">https://www.europarl.europa.eu/committees/en/aida</a>
- 2 Commission Communication on the European democracy action plan COM(2020) 790 final, EUR-Lex 52020DC0790 EN EUR-Lex (europa.eu)
- 3 European Commission, "Shaping Europe's Digital Future: The Digital Services Act package" https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
- European Commission, Joint Communication to the European Parliament, the European Council and the Council: "A new EU-US agenda for global change" (JOIN(2020) 22 final)
- 5 Speech by President von der Leyen at the World Leader for Peace and Security Award (12 December 2020) (SPEECH/20/2402)
- 6 European Commission, "A new EU-US agenda for global change" (JOIN(2020) 22 final), p.7
- 7 Biden, J. R., "Why America Must Lead Again: Rescuing U.S. Foreign Policy After Trump", Foreign Affairs (Issue: March/April 2020) <a href="https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again">https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again</a>
- 8 Feldstein, S., "How Should Democracies Confront China's Digital Rise? Weighing the Merits of a T-10 Alliance", Council on Foreign Relations (30 November 2020) https://www.cfr.org/blog/how-should-democracies-confront-chinas-digital-rise-weighing-merits-t-10-alliance

## **Key takeaways:**

#### Panel 1:

Technology reflects societal values, either implicitly or explicitly, and the future of democracy will depend on maintaining media plurality, the possibility for dissent, and a human-centric public discourse. When shaping the narrative on how to regulate platforms and new AI technologies, policy-makers must consider the entire context of public opinion formation, and the role not only of rationality, but also human empathy and emotionality. Lorena Jaume-Palasí (Executive Director, Ethical Tech Society and Founder, Algorithm Watch) also noted the importance of nuance in public discourse and online speech, highlighting the necessity of distinguishing between polarisation and radicalisation, and recognising that the appeal of disinformation is rooted in emotions and political affiliation, rather than rational belief in the veracity of facts.

The intersection of social media, political participation, and AI presents new challenges for both the tech sector and society as a whole. Yannis Theocharis (Chair of Digital Governance, Bavarian School of Public Policy, Technical University of Munich) presented academic research on how AI can be used to counter incivility, hate speech, and other forms of abuse on social media platforms such as Twitter. Research findings showed that while social media- enabled political participation could have positive democratic effects, such as the emergence of new social movements and agenda-setting "hash-tag activism", it could also lead to abusive rhetoric towards politicians and an overall impoverishment of public discourse. Whereas social media abuse affects all politicians, regardless of political affiliation, the research yielded results on how gender and other personal characteristics can impact the amount of abuse a politician received. Popular female politicians, with substantial social media followings, were likely to receive not only quantitatively more abuse than male politicians, but also gender-based abuse targeted specifically towards their personal characteristics.

The potential of AI to reduce the amount of abuse on platforms is inherently linked to problems of definition - how hate speech is defined varies across jurisdictions and platforms. The consequence is that there is limited consensus on how to harness AI to effectively filter out hate speech and incivility. Where problematic online behaviour can be defined and used to train AI systems, Al-based solutions can include automated content moderation, automated counter-speech, and automated nudging - prompting users to reconsider the language used before posting. A secondary problem arises in relation to the incentives of platforms to implement solutions that could harm profits. In many documented instances, uncivil or divisive language on social media leads to greater user engagement and more followers. The goal of reducing or removing uncivil and divisive content therefore appears to be in direct conflict with platforms' business models geared towards maximising user engagement.

Whereas the offline world has moved online, offline laws and standards have not been accordingly updated. The technology-driven amplification of misinformation over and above the types of information critical to democracy cannot be countered by a "whack-a-mole", after-the-fact type of content moderation, as explained by **Karen Kornbluh** (Senior Fellow and Director, Digital Innovation and Democracy Initiative, German Marshall Fund of the United States). Often spread by repeat offenders, salacious content and flagrant misinformation is taken down only when it is has already gone viral. As such, it distorts evidence-based news reporting and is disruptive to the national news cycle. Information critical to the survival of democracies cannot compete with the motivated disinformation propelled by increasingly influential platforms and Al-powered algorithms. A recent example is that of the Texas power outage being falsely linked to frozen wind turbines. When acting to counter disinformation and penalise the outlets in question, governments and law makers ought to look towards both existing solutions, such as the application of consumer protection or harassment laws online, as well as future-oriented Al-based solutions, coupled with robust capacity-building, training, and government oversight.

As new technologies and new forms of media emerge, existing models of governance - including democracy - are being challenged. New informational technology fundamentally rewires societies and technology's effect on governance cannot be underestimated. Coupled with disintermediation, a truth crisis and a perception crisis are emerging, amplified by the persuasive power of new AI applications that can lead to a paralysing information asymmetry that threatens democracies, according to Aza Raskin (Co-founder, Center for Humane Technology and Earth Species Project). Increasingly, using AI, tech platforms such as Google, Facebook, and Twitter have more information on a person's identity and knowledge of their decisional history than traditional fiduciary-bearing personal advisors such as doctors, lawyers, or bankers. Often, such data is gathered in ways which do not violate existing privacy norms, but are used for predicting outcomes in a manner which is unknown or misunderstood by the user and the general public. The protection of fundamental democratic values such as freedom of expression and human dignity can no longer be guaranteed, and democratic models of governance are increasingly in competition with digital authoritarianism that is emerging as a viable alternative model. A promising solution may lie not in trying to stem the tide of misinformation and polarisation, but using technology to optimise for content which allows us to see the other side of a societal debate more directly, without distortion. This would allow for the bridging of the gaps in perception which often lead to divisiveness and polarisation.

#### Panel 2:

In the new media ecosystem, everyone is a consumer - and new forms of user generated content (UGC) are changing the very definition of media, according to **Anna Bulakh** (Director, Disinfo.Tech and Co-Founder, Cappture.cc). UGC technologies are being developed at ever-increasing speed; while in 2019, an estimated 14,000 deep fake videos were in circulation online, by 2020 that figure had risen to about 4 billion, following the virality of certain UGC-driven apps. The mass use and consumption of synthetic media is linked to increased vulnerabilities, misinformation, disinformation, and criminal operations. The commodification of AI and deep learning tools is resulting in a surge of inauthentic content and markedly changing the media landscape. An accountability ecosystem driven by harmonised standards and coupled with the education of both users and regulators will be key to empowering creators and protecting consumers of new types of synthetic media in the creative economy. International consensus is urgently needed on how content - whether text, photo, audio, or video - is marked as well as on common standards on metadata, authenticity and transparency.

Whereas there has been a seismic shift in the way disinformation and influence operations have evolved in recent years, many democracies retain a 2016 mind-set. According to research carried out by the Stanford Internet Observatory as presented by Alex Stamos (Director, Stanford Internet Observatory), the vast majority of online disinformation and political interference is conducted by domestic- not foreign - actors. At the time of writing in 2021, the most effective mechanisms of political interference are the "injection of an idea" into the political discourse followed by its amplification by domestic political elites and subsequent obscuring of the initial source. Such tactics are often combined with sophisticated cyber capabilities, or the use of local proxies by foreign operators to spread locally created - and therefore often more credible - disinformation. "Hybrid" attacks on democracies must be countered by a better understanding of both cyberattacks and hacking. A report by the Election Integrity Partnership (EIP), a nonpartisan coalition of misinformation researchers, found that the most active spreaders of disinformation were domestic actors with large social media followings. Disinformation shared by such domestic "multimedia stars" can be picked up by traditional media outlets in a manner that presents significant new challenges for both regulators and tech platforms. Fighting disinformation will increasingly become a trade-off between sovereignty and privacy. In this regard, focus perhaps needs to shift from seeing algorithms and algorithmic amplification as the main and only problem (nor, conversely, as a "silver bullet" solution) but rather enlarging the debate to better address the human behaviour, political rhetoric, and the daily choices made by both creators and consumers of content, who are ultimately the source of much of the disinformation and misinformation that is circulated.

While representing a very real and serious threat to democracies, current research on disinformation and fake news shows that much of it is both consumed and disseminated by very small, highly motivated and often highly partisan minorities, according to Rasmus Kleis Nielsen (Professor of Political Communication, Oxford University). Recent findings of the Reuters Institute relating to the US content have shed light on this evolving phenomenon, and showed that while news consumption accounts for 15 percent of daily media consumption by Americans, only 0.15 percent comprised fake news. In the modern media environment, there are various other forms of network propaganda and problematic information, including but not limited to hyper-partisan material, harassment, and trolling - especially of women, ethnic minorities, and marginalised communities. In terms of public perceptions of foreign interference and disinformation, surveys conducted across nationally representative samples of internet users across twenty EU Member States showed that the majority of respondents (38%) identified their own governments, domestic politicians, or national political parties as being the most concerning source of potentially false and misleading information. These findings are important as the effectiveness of any policy response will ultimately depend on public perceptions, and much of the available research in this area points to such perceptions as often being accurate and backed by evidence.



# **Contributions by Political Groups**

#### Disclaimer:

The statements herein below are drafted by the political groups of the European Parliament. The opinions expressed are the sole responsibility of the author(s) and do not necessarily represent the official position of the European Parliament. This document may contain links to websites that are created and maintained by other organisations. The AIDA Committee and the AIDA Secretariat do not endorse, nor are they affiliated with, the view(s) expressed in the said statements nor through the said websites.



#### The European People's Party Group (EPP)

The EPP Group believes that shaping a fair digital environment, including AI technologies, has to be characterised by democratic values such as respect for fundamental rights, including protection of privacy and personal data, the principle of non-discrimination, freedom of expression and information, media freedom and pluralism.

It is of outmost importance to reap the socio-economic benefits that AI technologies offer for open and democratic societies. The EPP Group believes that a clear strategy is needed in order to mitigate risks to democracies associated with AI technologies, such us facilitating the spreading of hate speech, disinformation, illegal content, bias against groups in vulnerable situations, cyber-crimes or manipulating choices in economic and political decisions. We believe that any regulatory approach has to be proportionate and human-centric, as well as encompass such elements as users' safety and respect for their fundamental rights, strong and robust compliance systems, and enforcement. It should be topped-up by targeted awareness-raising campaigns on AI's advantages and risks for civil society.



#### The Progressive Alliance of Socialists and Democrats Group (S&D)

Al must be ethical and democratic in order to be future-proof. Al needs the citizens' trust based on democratic oversight and digital literacy. In order to prevent Al technologies from undermining democratic processes, Al must fully respect fundamental rights, in particular the freedom of expression and opinion; on the other hand, the EU needs to address the spread and impact of hate speech, and misleading or false content. Al-powered solutions to disinformation, such as automated counter-speech and automated nudging, must be based on strong evidence before their eventual use, and they cannot replace legislation but can only complement it. The EU must promote digital and media literacy education to empower citizens to analyse the quality and relevance of information sources. Certain Al systems should be classified as high-risk, due to their potentially significant impact on democracy, rule of law and individual freedoms, such as Al systems intended for the administration of justice and democratic processes. Globally, the EU should lead a regulatory process that promotes our democratic values and principles, working closely with its like-minded partners towards an international agreement for an ethical and democratic Al in the world.

# renew europe.

### The Renew Europe Group

Artificial intelligence offers great opportunities for our society and economy alike. We need to guarantee that AI technologies are developed and deployed according to our democratic rules and values, ensuring full respect for individual freedoms, human rights, and the rule of law. However, AI technologies can also be used in a harmful way. Authoritarian regimes are already applying AI systems to control, spy, monitor and score citizens. We cannot allow emerging technologies to be misused in a similar manner within the EU, nor that they are utilized to destabilise our societies, undermine our democracies and electoral processes, or manipulate and disinform our citizens. We must set up clear rules in order to ensure that AI is not used for undemocratic purposes such as mass surveillance and mass social scoring by European governments. In addition, developers and deployers that can influence these processes should be bound by ethical principles. We should also reach out to democratic partners around the world in order to work together, building an alliance to set international standards for AI. Moreover, we need to strengthen our cybersecurity, increase our citizens' resilience to fake news and disinformation through education, and enhance digital knowledge and skills.



#### ID

Disinformation - the dissemination of verifiably false or misleading information for deceiving the public - may endanger the correct evolution and application of democracy. This threat is particularly dangerous when foreign governments deploy disinformation as one of the soft power tools, besides diplomacy and communications operations, to influence the democratic evolution of a legitimate government.

Younger people are more likely to obtain news online, through social media, direct outlet or direct search, and so they are more influenced by a foreign power's possible malicious operations. Even inside the European Union, we had seen cases, like in Poland, of direct disinformation operations aimed to damage public trust in the institutions.

The future of democracy is directly linked to the balance between freedom of speech and contrast to the diffusion of fake news and misleading information, especially when they are a tool in the hands of an external actor. Usually, the public is more concentrated on false or misleading information coming from domestic politicians or news media, but we have to focus more on the threat coming from external actors aimed at debasing the roots of our democracy.



#### **Greens/European Free Alliance**

Today a growing number of innovations are based on large-scale data collections from digital devices and real-time access to information. Media plurality, human centric public discourse, together with a robust civil society are fundamental to ensuring that the current digital revolution will bring about more resilient liberal democracies. Undemocratic practices such as mass surveillance, mass social scoring by the state, or discrimination in Europe should be fought against by all governments, and fundamental rights as well as freedom of expression must be ensured. In order to reduce harmful and divisive content we must question the current business model of big tech platforms rather than further increasing their power. Europe must set rules, standards, and red lines of a digital future worldwide and guarantee that the potential of new technologies is fully achieved, while transparency and democratic participation as well as redress are improved.



#### The Left

Al-driven solutions will disproportionately affect the most vulnerable in society, such as workers, minorities and women, and pave way for new power asymmetries and exploitation. In order to reduce Al bias, their voices must be put on the forefront of Al development so that their rights are properly taken into account. Democratic values such as labour rights, inclusion, fundamental rights and human dignity must be respected. The rise of 'digital authoritarianism' supported by the oligopolistic power of Big Tech platforms is a big threat for democratic societies. On one hand, Al can play a positive role in filtering online content and disinformation, but a proper democratic scrutiny is required for citizen empowerment. To this end, future Al legislation should focus on labour and fundamental rights, rule of law and democracy. We are gravely concerned that the European Commission's new proposal emphasising global innovation ahead of human rights protection, leaves the most vulnerable to be negatively affected. As supported by 56 civil society organisations and 116 MEPs, we also call for a complete ban on undemocratic biometric mass surveillance and facial recognition.

