Economic and Social Council

Tackling Democracy in a Digitalised World

Lycée Franco-Allemand Buc
Deutsch-Französisches Gymnasium Buc

JEAN MONNET HOUSE

LFA EuroMUN

Table of Contents

Introduction

Ever since the Digital Revolution, also known as the Third Industrial Revolution, which began in the latter half of the 20th century, the world has been rapidly digitalising. These new technologies have created and will continue to create new ways to share information, govern, and live. This poses new opportunities but also new threats to the democratic world. With the rapid development of technologies such as artificial intelligence (AI), governments will have to create laws to regulate the technology, from the use of facial recognition for mass surveillance to the misuse of data, among others. Another key aspect of this debate is the manipulation of information on platforms, notably social media platforms, as well as the influence of private companies on the choice of information being presented to citizens. In a world where disinformation is widely present, it is imperative that reliable information be safeguarded and made equally available to all, as it is a key part of democracy. The use of cyberattacks to destabilise democracies will also be at the centre of this debate. Delegates will have to offer solutions to address the problems caused by these new technologies to ensure that democracy remains and thrives.

Definition of Key Terms

Democracy

Government by the people, exercised either directly or through elected representatives. The United Nations does not advocate for a specific model of government but promotes democratic governance as a set of values and principles that should be followed for greater participation, equality, security and human development.

Digitalisation

The integration of digital technologies into everyday life. Digitalisation can be present in a variety of sectors, such as trade, economics or politics.

Transparency

An environment of openness where the access and disclosure of information is a matter of principle and human rights. Leaders, officials and those in power operate in a visible and predictable manner that promotes trust and participation. Transparency is widely understood as a necessary precondition to prevent corruption and promote good governance and sustainability.

Fake News

Fake news or information disorder is false or misleading information presented as real news. It often has the aim of damaging the reputation of a person or entity. Misinformation, disinformation, malinformation, propaganda are all forms of fake news.

Misinformation

Misinformation refers to false information that is not intended to cause harm.

Disinformation

Refers to false information that is intended to manipulate, cause damage, or guide people, organisations, and countries in the wrong direction.

Malinformation

Refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm.

Propaganda

Information, especially of a biassed or misleading nature, used to promote a political cause or point of view.

Hate Speech

Hate speech refers to offensive discourse targeting a group or an individual based on inherent characteristics (such as race, religion or gender) and that may threaten social peace.

Political Paralysis

Political paralysis refers to the delays, inaction and inability to take policy decisions by the government or its various departments and agencies which runs the country and the economy.

Echo Chamber

Because social media platforms mostly depend on advertising for revenue, and because targeted advertisements can be sold for more expensive than non-targeted advertisements, social

media platforms profit from polarising users into distinct categories by showing them a vast majority of media relating to these distinct categories. Furthermore, people tend to interact more with media that elicits strong emotions, leading social media platforms to promote pieces of media that are considered shocking or extreme in the opinions they share. In these categories, or echo chambers, users only encounter information or opinions that reflect and reinforce their own. Echo chambers can distort a person's perspective so they have difficulty considering opposing viewpoints and discussing complicated topics. The disproportionate role of social media platforms in influencing citizens' opinions poses the questions concerning democracy and control of the media.

Digital Divide

The gap between the people who have access to modern information and communications technology and those who do not.

Cyberattack

A cyberattack is an attempt by hackers to destroy a computer network system. Cyberattacks are an important threat against democracies as cybercriminals, as well as possible state-funded cyberattacks, can use a wide range of different tools to destabilise democracies. The following definitions are examples of cyberattacks that can target governments and potentially destabilise democracies.

Malware

A software that is specifically designed to disrupt, damage or gain unauthorised access to a computer system.

Distributed Denial of Service (DDoS)

Cyberattack, which overloads a system or network with excessive traffic, making it unavailable to users.

Phishing

A deceptive attempt to obtain sensitive information by posing as a trustworthy entity through emails and messages.

Ransomware

A malware that permanently blocks access to a victim's personal data unless a ransom is paid.

Advanced Persistent Threats (APTs)

Long-term, targeted cyberattacks, often state-sponsored, aiming to steal information.

General Overview

Transparency

Transparency in democratic countries has greatly grown, with platforms such as social media allowing citizens to have easier access to information. In today's world, knowledge is easily and constantly accessible through online articles, infographics, video explanations, broadcasts of meetings, digitalisation and cataloguing of archival documentation, social media posts, and more. However, the validity and reliability of the information is not guaranteed and sources can be hard to trace. This is notably a problem occurring with the growing use of AI.

Pluralism

Additionally, media freedom and pluralism, which is an essential part of democracy, can be threatened online, notably through abuse of defamation laws, intimidation, or pressure, which damage the environment in which journalists work. Journalists can also be the targets of cyber harassment and hate speech, which can lead to self-censorship and reduce the scope of public debate online. Furthermore, as social media grows, citizens tend to move away from traditional media, making the regulated job of journalists near obsolete.

Elections

Elections are vulnerable to cyberattacks and electoral manipulation due to their periodic nature and the growing digitalisation of this legislative process. Their advanced scheduling makes it easier to plan attacks, hack into registration databases, tamper with the vote tabulation systems, spread malware to disrupt voting machines, etc. Furthermore, social media's influence on the media citizens have access to allows private companies to greatly influence citizens' political opinions by selecting the information and media to show each user, thus jeopardising democracy. Another threat

to democratic elections is the spread of disinformation, especially by foreign powers. This can cause decay of public trust in governmental institutions, decay in civil public discourse and political paralysis. The global scale of digitalisation and particularly of social media allows the quicker spread of information and therefore amplifies the impact of electoral propaganda. Disinformation as well as hate speeches makes it so that monitoring of social media is greatly needed. Overall, digitalisation makes it easier to manipulate election outcomes through a variety of different means.

Artificial Intelligence

Artificial intelligence is a new and growing technology. Today, AI is being used by governments to expand or replace law enforcement functions, assist in public benefit decisions, and intake of public complaints and comments. Though it has many advantages, AI is also an important threat to democracy as it can pose problems with data privacy, facial recognition technology as well as misinformation, and its use is still poorly regulated. Authoritarian regimes have seen AI as an opportunity to control their population more, as well as a way to undermine democracy. This is why regulations on the subject of AI are very important.

Active Citizenship

Finally, digitalisation brings shifts in active citizenship. Through digital platforms, different communities gain a voice and means to participate in civic discourse, promoting inclusivity. Social media facilitates organization and mobilization of citizens around causes, fostering timely responses to societal issues. Moreover, digital tools empower citizens to hold governments and institutions accountable by exposing corruption and injustices, promoting transparency. However, digitalisation also presents challenges. These include the digital divide which favours citizens with access to technology and internet, echo chambers, misinformation, cybersecurity threats, and shallow engagement. These issues hinder constructive dialogue, erode trust in institutions, and compromise the safety and privacy of activists.

Major Parties Involved

The GAFAM

Google (Alphabet), Apple, Facebook (Meta), Amazon, and Microsoft, commonly known as GAFAM, are the five largest US tech companies. These companies possess an unparalleled collection of user data which is the most extensive in the world, and they are in a unique position to evaluate

this data by means of algorithms and to determine what information is presented to the users of their services. Their power to influence citizens' political views therefore raises many questions in democracies worldwide.

For instance, using data from over fifty million Facebook profiles without the users' consent, the British tech firm Cambridge Analytica provided analytical assistance to the 2016 presidential campaigns of Ted Cruz and Donald Trump. By microtargeting users with curated information based on their personality and the media they like to consume, Cambridge Analytica could distort the political opinions of millions of voters without their noticing. While traditional media shares the same information with everyone, the GAFAM has the power to create specific content which will be shown only to certain people and not to others, giving the five CEOs of the GAFAM disproportionate power over democracies worldwide.

China

In the past few years, the People's Republic of China (PRC) has felt more and more threatened by democracies while autocracies around the world fall. As it feels increasingly pressured by its democratic neighbours, China has resorted to a variety of anti-democratic tools such as non-governmental organisations, media outlets, hackers, et caetera to prop up dictatorships and destabilise democracies. China works with fellow authoritarian regimes like Russia to push autocrat-friendly norms of internet management on international institutions. China is also known to spread disinformation and propaganda on social media. The nation is pioneering a system that will allow dictators to have more complete knowledge of their subjects using AI, "big data" and facial-recognition technologies. This is an important threat to democracies as China implements this system in their own nation and helps other authoritarian regimes implement it in theirs.

Russia

Russia has been accused of sowing social discord and interfering in elections, especially in western democracies such as the United States of America, the European Union, and Ukraine. The Russian Federation has exploited pre-existing political polarisation to undermine democracies as well as targeted cyberattacks such as but not limited to a phishing attack during the American presidential election of 2016, and DDoS attacks during the Ukrainian presidential election of 2014. Russia has also conducted large campaigns of disinformation, utilising social media to influence public opinion.

The United States of America (USA)

As one of the foremost democracies in the world, the USA prioritises cybersecurity measures to protect critical infrastructure, especially its election systems. Diplomatically, the USA is globally engaged to counter disinformation campaigns, deploying sanctions and fostering international collaboration. The country actively monitors social media platforms, collaborating with tech companies to identify and remove misleading content. Overall, the USA seeks to fortify its democratic institutions and contribute to global efforts in countering disinformation. The USA especially participates in counter-espionage and tries to thwart foreign attempts to interfere in its elections.

The European Union (EU)

Similarly to the USA, the EU is a leader in cybersecurity and countering disinformation. The EU has a commitment to empowering citizens through education and awareness of social media and the Internet in general. Through legislative measures, the EU aims to promote transparency, accountability, and ethical practices in the use of technology. This approach seeks to strike a balance between technological innovation and safeguarding democratic principles, ensuring that digital platforms operate within ethical boundaries. The EU also advocates global norms for digital technologies and strengthening the democratic use of these technologies.

Timeline of Key Events

Estonian Parliamentary Election (2007)	Estonia faced a series of cyberattacks, including DDoS attacks, during its parliamentary elections. The attacks targeted government websites, online news outlets, and banks, causing disruptions and raising concerns about the vulnerability of critical infrastructure.
Operation Aurora (2009-2010)	This was a series of cyberattacks led by China to steal intellectual property and sensitive information from many American companies in 2009 and 2010. This raised many concerns on the use of cyberattacks to destabilise western democracies.
Ukraine presidential election of 2014	After Russia's annexation of Crimea, there were great fears that it would try to tamper with the election through cyber interference. The

	Ukrainian Central Election Commission reported many DDoS attacks on its servers, potentially affecting the availability of the website and disrupting communication and report processes.
US presidential election of 2016	This election was subject to multiple disinformation campaigns, especially on social media, but was most notably affected by phishing attacks which allowed cyber criminals associated with Russia to steal data from various actors, including the Democratic Congressional Campaign Committee.
Wannacry Ransomware Attack (2017)	This ransomware attack was a worldwide cyberattack which impacted many organisations, most notably the National Health Service in the United Kingdom.
March 2018	Whistleblower Christopher Wylie exposed Cambridge Analytica's role in influencing the US Presidential Elections of 2016.
Network and Information Systems Directive (2018)	The NIS Directive focuses on improving cybersecurity in the EU.
General Data Protection Regulation (2018)	GDPR is an EU regulation addressing data protection and privacy for individuals in the EU.
Digital Services Act (DSA) and Digital Markets Act (DMA) (2020)	These regulations aim to create a safer digital space in the EU. DSA focuses on content moderation and tackling disinformation, while DMA aims to regulate large online platforms.
European Democracy Action Plan (2020)	This plan outlines measures to protect and strengthen European democracy, especially in addressing disinformation, transparency in political advertising and cooperation with online platforms.
AI Regulation Proposal (2021)	This regulation aims to create a legal framework for artificial intelligence in the EU. It addresses aspects such as transparency, accountability and human oversight on the subject of AI.

Previous Attempts to Resolve the Issue

European White Paper on Artificial Intelligence (2020)

This focuses on the creation of a regulatory framework for AI to maximise the opportunities brought by this technology while minimising its risks. This includes:

- Regular control of the use of AI to ensure that it respects the Charter of Fundamental Rights of the European Union, the Treaty on the Functioning of the European Union and secondary Union law. These clauses not only concern AI but also robotics and related technologies including software, algorithms and data used or produced by such technologies
- The creation of a common EU data space to ensure the respect of EU data protection rules
- Transparency on the use of AI and the filtering, accuracy and limitations of information provided

EU Cyber Defence Coordination Centre (EUCDCC)

This centre was created to increase situational awareness and increase early detection capacity, as well as improve resources to respond properly to any attacks and recover in a solidary and coordinated manner. This centre is part of the EU's policy on Cyber Defence.

European Democracy Action Plan (2020)

This action plan aims to protect democracy from the downfalls of digitalisation. It notably touches upon:

- The transparency of political advertising and campaigns, notably the transparency of sponsored political content to provide legal certainty and ensure that the respect of fundamental rights and standards are upheld online
- The transparency on the financing of European political parties, and the creation of new operational EU mechanisms to support resilient electoral processes, monitor threats, particularly those relating to cyberattacks, and ensuring cooperation in the EU to ensure free and fair elections
- The strengthening of the knowledge base online to help citizens and national electoral authorities build resilience against threats, such as foreign threats or disinformation
- An initiative to extend the list of EU crimes to cover hate crime and hate speech, including online hate speech

- An improvement on the Code of conduct on tackling illegal hate speech online which has been followed by platforms such as Facebook, Instagram, Snapchat and TikTok
- Strengthening media freedom and media pluralism along with protecting journalists from cyberharassment and hate speech through the creation of a Platform to Promote the Protection of Journalism and Safety of Journalists
- Strengthening cooperation structures within the EU and with international partners to fight disinformation, and to strengthen the resilience of third countries to counter foreign influence and disinformation
- Monitoring the impact of disinformation and the effectiveness of platforms' policies
- Improving fact-checking on social media platforms

Possible Solutions

Digital Literacy and Education

Establishing courses to educate future citizens on topics such as the evaluation of online information, the implications of digital footprints, the advantages and downfall of AI, et caetera. This can be accompanied by increased education about European values, such as freedom of speech, transparency, and democracy, these values being relevant in today's digitalised world. These learning programs could be integrated in schools' curricula.

Tackling AI Biasses

Reviewing current AI learning programs to enable the fairer functioning of this technology. This would allow AI to be used in a safer manner in governmental activities, and cease the current increase of discrimination and prejudice due to the unregulated use of AI.

Civil Participation

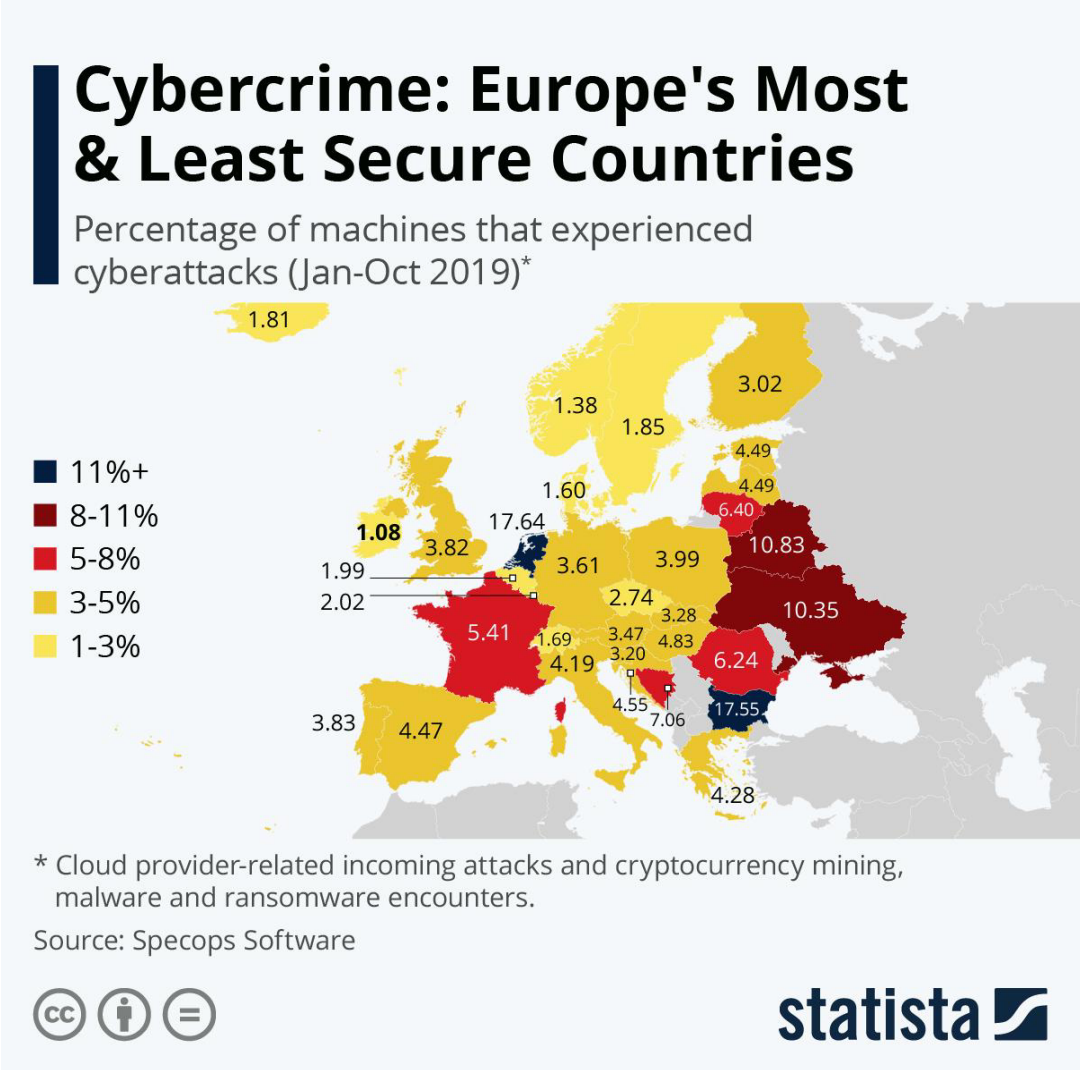
The creation of online forums, digital platforms, et caetera to encourage online civil participation in democratic matters. The setting up of feedback systems, awareness campaigns, electronic petition systems, or participatory budgeting tools, all online, are new digital ways to increase civil involvement and consequently strengthen democracy.

Equal Access to Technology

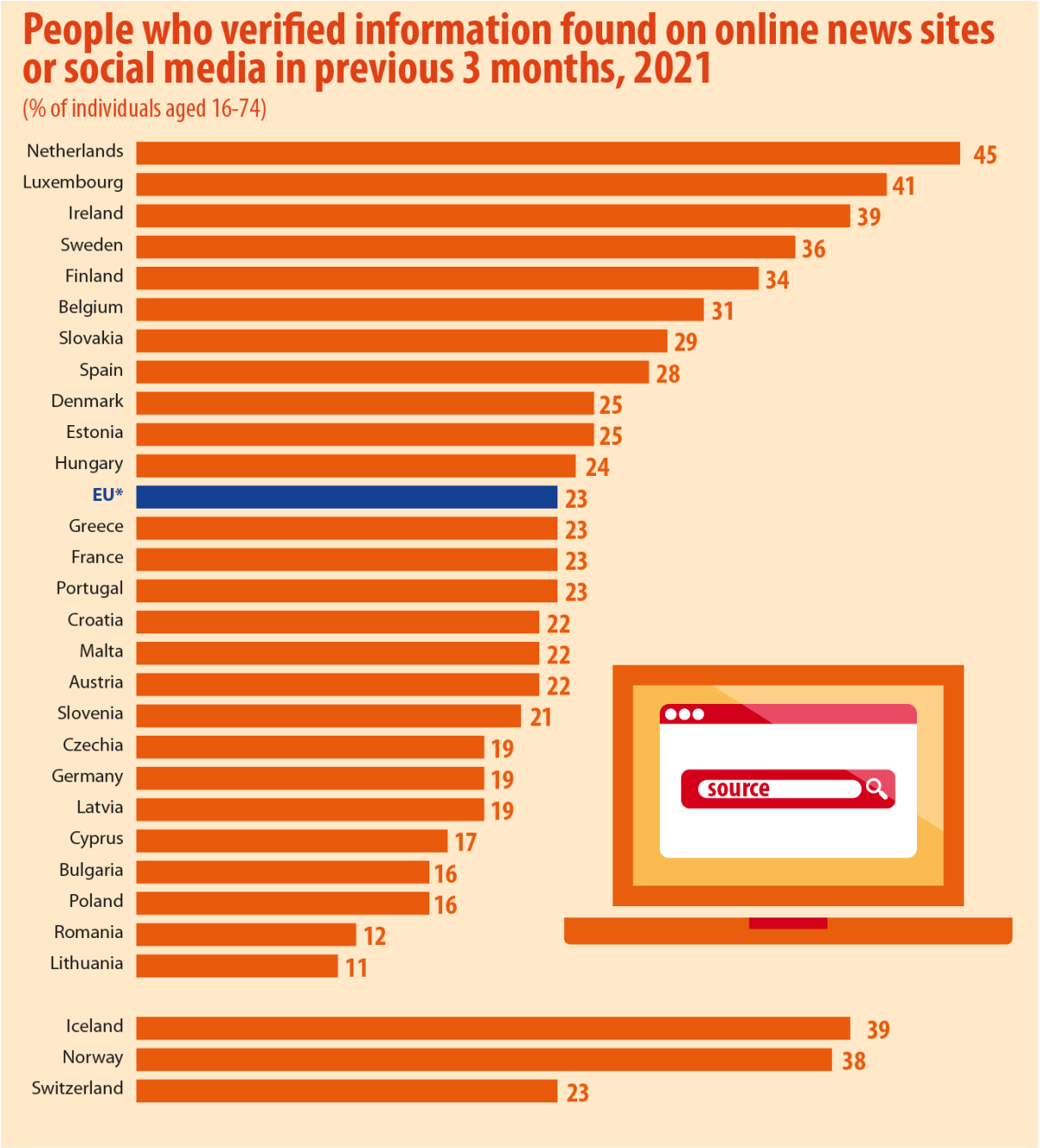
With the digital divide halting the active citizenship of poorer citizens, it is important to ensure equal access to technology for all. This can mean subsidising internet access, increasing the development of technological infrastructure, establishing community centres to give low-cost access to technology and internet, or encouraging device recycling.

Appendices

Appendix A



Appendix B


People who verified information found on online news sites or social media in previous 3 months, 2021
(% of individuals aged 16-74)
Netherlands 45
Luxembourg 41
Ireland 39
Sweden 36
Finland 34
Belgium 31
Slovakia 29
Spain 28
Denmark 25
Estonia 25
Hungary 24
EU* 23
Greece 23
France 23
Portugal 23
Croatia 22
Malta 22
Austria 22
Slovenia 21
Czechia 19
Germany 19
Latvia 19
Cyprus 17
Bulgaria 16
Poland 16
Romania 12
Lithuania 11
Iceland 39
Norway 38
Switzerland 23
source
*Italy: data not available. As a result, the EU aggregate has been estimated.
ec.europa.eu/eurostat

Bibliography

European Parliament. “Digital Democracy”. 2020. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646161/EPRS_BRI(2020)646161_EN.pdf

Hamilton, Robert E.“Russia's Attempts to Undermine Democracy in the West: Effects and Causes” 2019. https://www.sciencedirect.com/science/article/abs/pii/S0030438719300663

Beckley, Michael and Brands, Hal. “China’s Threat to Global Democracy”2022. https://www.journalofdemocracy.org/chinas-threat -to-global-democracy/

European Commission. “Data protection in the EU”. 2018. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

European Parliament. “EU AI Act: first regulation on artificial intelligence”. 2023. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

EUR-Lex. “Democratic Deficit” https://eur-lex.europa.eu/EN/legal-content/glossary/democratic-deficit.html

European Parliament. “Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies”. 2020. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html#title1

World Economic Forum. “Here’s What to Know about Elections, Cybersecurity and AI”. 2023. https://www.weforum.org/agenda/2023/11/elections-cybersecurity-ai-deep-fakes-social-engineering/

Electronic Privacy Information Center. “Outsourced & Automated”. 2023. https://epic.org/outsourced-automated/

European Commission. “The EU Code of Conduct on Countering Illegal Hate Speech Online” https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

European Commission. “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions”. 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790

Ministère de l’Enseignement Supérieur et de la Recherche and Horizon Europe. “Digital Democracy” https://www.horizon-europe.gouv.fr/digital-democracy-32239#:~:text=However%2C%20digital%20solutions%20are%20also

Eike, Elisabeth. “Digitalization and democracy Fake news, disinformation and the EU”. 2020. https://www.eu3d.uio.no/publications/eu3d-reports/eu3d-report-2-eike.pdf

European Parliament. “Civil liability regime for artificial intelligence”. 2019. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.pdf

Karásková, Ivana, and Bērzina-Čerenkova, Una Aleksandra. “Foreign Electoral Interference Affecting EU Democratic Processes”. 2023. https://www.appf.europa.eu/cmsdata/277388/Foreign%20electoral%20interference%20affecting%20EU%20democratic%20processes.pdf

European Partnership for Democracy. “A comprehensive plan to innovate democracy in Europe” https://www.youthforum.org/files/a-civil-society-vision-for-the-european-democracy-action-plan-input-paper.pdf

United Nations. “What is hate speech?” https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech

Canadian Centre for Cyber Security. “How to identify misinformation, disinformation, and malinformation”. 2022. https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300

Pavuluri, Prudhvi. “Policy Paralysis”. 2013. http://socialsciences.in/article/policy-paralysis

Electronic Privacy Information Center. “Government Use of AI” https://epic.org/issues/ai/government-use-of-ai/

Encyclopædia Britannica. “Transparency”. 2019. https://www.britannica.com/topic/transparency-government

Cadwalladr, Carole and Graham-Harrison, Emma. “50 million Facebook profiles harvested for Cambridge Analytica in major data breach”. 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election