

Artificial Intelligence and Democratic Elections – International Experiences and National Recommendations

Report by the Expert Group on Artificial Intelligence and Elections

February 2025

(Translated version)



To the Ministry of Local Government and Regional Development

The Expert Group on Artificial Intelligence and Elections was appointed by the Ministry of Local Government and Regional Development on 6 June 2024. The Expert Group has been tasked with assessing the significance of artificial intelligence for secure and democratic elections and propose measures to meet the challenges it poses to Norwegian democracy and to ensure confidence in Norwegian elections. The Expert Group expresses its gratitude to all who have contributed to this work.

The Expert Group hereby submits its report.

Oslo, 5 February 2025

Niels Nagelhus Schia
(Chair)

Anne Sofie Molandsveen

Helle Sjøvaag

Rune Karlsen

Bente Kalsnes

Julie Ane Ødegaard Borge

Heidrun Åm

Lars Raaum

Øyvind Kind Robertsen
(Head of Secretariat)

Vilde Sollien

Summary	6
1 The Expert Group’s mandate, composition, and work	9
1.1 Background for the Expert Group.....	9
1.2 Mandate	10
1.2.2 The Expert Group’s interpretation of the mandate	12
1.3 Composition.....	13
1.4 The work of the Expert Group	13
1.5 Key terms	14
2 Technology, media, elections, and democracy – the situation in Norway	16
2.1 Security policy situation	16
2.2 The election process in Norway	17
2.2.1 Roles and responsibilities.....	17
2.2.2 Use of technology in the election process.....	17
2.2.3 Security efforts in connection with elections.....	18
2.2.4 Voting patterns and variations in voter turnout	19
2.2.5 Election campaign.....	20
2.3 Media and technology use in Norway	21
2.3.1 Editor-controlled media and its use	21
2.3.2 Social media and its use	22
2.3.3 Norwegians’ familiarity with and use of AI	24
2.3.4 The role of media in election campaigns.....	26
2.4 Democracy and trust.....	27
2.5 Norway’s digital infrastructure	29
2.6 Legislation and regulation of AI.....	30
3 What impact could AI have on elections?.....	34
3.1 The information and media landscape.....	35
3.2 Covert election influence	38

3.3	The election process and cybersecurity	41
4	Lessons learnt from elections conducted in 2024.....	43
4.1	Romania	44
4.2	Finland	46
4.2.1	Pre-election preparations in Finland.....	46
4.2.2	Events and lessons learnt from the election in Finland.....	46
4.3	Elections to the European Parliament	47
4.3.1	Preparations for the European Parliament elections	47
4.3.2	Events and experiences from the European Parliament elections ...	49
4.4	The United Kingdom.....	53
4.4.1	Preparations prior to the election	53
4.4.2	Events and lessons learnt from the UK election	54
4.5	The United States	57
4.5.1	Preparations prior to the elections	57
4.5.2	Events and lessons learnt from the US election.....	58
4.6	Individual events from other elections.....	63
5	Changes in the challenges facing Norwegian elections.....	67
5.1	The information and media landscape.....	67
5.1.1	Increased levels of misinformation and disinformation and reduced trust in information.....	69
5.1.2	Changes in sources of information used	70
5.1.3	Misrepresentation of persons and events.....	72
5.1.4	Greater dependence on powerful technology companies and platforms.....	74
5.1.5	A more algorithm-driven distribution of content.....	75
5.2	Covert election influence	76
5.2.1	Increased power and scale	77

5.2.2	A growing number of threat actors.....	77
5.2.3	Increased personalisation of influence operations	78
5.2.4	Increased polarisation and exploitation of divisive issues.....	78
5.2.5	Weakness in democratic preparedness that can be exploited.....	79
5.3	The election process and cybersecurity	79
5.3.1	Increased digital vulnerability.....	80
5.3.2	Increased grounds for speculation about errors or fraud in the election process.....	82
5.3.3	Gaps in AI expertise within public administration and politics.....	83
6	Summarised assessments and recommendations by the Expert Group.....	84
6.1	The Expert Group's recommendations.....	85
	References.....	90
	Appendix 1: Overview of whom the Expert Group met with and received input from.....	105

Summary

A comprehensive approach to artificial intelligence (AI) is required in order to safeguard the integrity of elections and to promote democracy at a time of rapid technological development. Although AI has equipped us with powerful tools with a variety of valuable applications, there is also a potential for misuse.

The Expert Group on AI and Elections was by the Ministry of Local Government and Regional Development to assess the significance of AI for democratic elections and to propose measures to meet the challenges posed by AI in this context. The work of the Expert Group has explored three primary areas of concern: (1) the information and media landscape, (2) covert election influence, and (3) the election process and cybersecurity.

The Expert Group emphasises that Norwegian society has a solid foundation for resilience against threats to democracy, which must be further developed and reinforced. With a diverse array of independent editorial media outlets, the Norwegian media system provides a firm foundation for resilience against rising polarisation and deepening fragmentation in society, as well as unwanted influence from AI-generated content in general, and AI-driven influence operations in connection with elections. Nevertheless, there are also signs that editorial media in Norway are under pressure from social media and shifting media consumption habits, particularly among young people.

Algorithm-driven systems have transformed the information landscape by enabling rapid and widespread distribution and dissemination of content on social media. The manner in which this occurs risks reinforcing personal beliefs while reducing exposure to a broader range of viewpoints. Social media have become increasingly important channels for information sharing, while editorial media face growing challenges in reaching the entire breadth of society. This contributes to a more nebulous information and media landscape.

Advances in AI, particularly large-scale language models, have raised concerns about their potential to generate false information and enable more sophisticated and covert influence operations. To date, AI has mainly contributed to reinforcing existing threats. However, the Expert Group believes it is important to ensure necessary democratic preparedness, societal resilience and AI competence among the authorities, including the intelligence and security services. Technology and trends are rapidly evolving – as are the challenges.

The elections examined by the Expert Group in 2024 reveal that the combination of AI, social media, and cyber operations has provided both foreign and domestic actors with

new opportunities to exert covert election influence. A particularly disconcerting and illustrative example of this is the Romanian presidential election.

AI-generated content garnered significant attention in the 2024 election year, especially in the United States. This shows that generative AI can have a discernible impact on the pre-election political agenda. The veracity of the content appears less significant in determining whether it achieves widespread dissemination as long as it reinforces or represents the recipient's opinions or perception of reality.

There is no available overview of the reach and potential of such technology, nor of how it will impact society and individuals over time. In its work on this report, the Expert Group has identified some changes in the challenges facing Norwegian elections. These changes align with the primary areas of concern and highlight where AI can significantly alter or reinforce challenges that warrant particular attention.

The Expert Group presents several recommendations based on insights gathered from elections held in 2024, combined with knowledge of AI usage and Norwegian conditions. The recommendations aim to mitigate the risk of AI being used in ways that adversely affect elections and democracy. To address the changes to the overall challenges, the Expert Group submits the following overarching recommendations:

- Ensure that the electoral authorities possess the necessary competence and capacity in AI and communication.
- Reduce the basis for speculation regarding errors and deficiencies in the election process or that the election is subject to unwanted influence.
- Contact between the authorities and the technology and platform companies.
- Political actors should be made responsible and supported.
- Prioritise the rapid implementation of relevant EU legislation, especially the Digital Services Act and the AI Act.
- Pursue an active media policy that maintains an independent, strong and diverse editorial media.
- Build source awareness and promote critical media, digital, and AI literacy skills.
- Increase research and cooperation between authorities, researchers, civil society and technology companies.
- Act as a driver for international cooperation in the above-mentioned domains.

The recommendations are further elaborated and discussed in section 6.1 of the report.

The Expert Group believes these recommendations will help enhance awareness and preparedness among the population, as well as among the authorities involved in the election process, the media, and technology companies. At the same time, the Expert

Group warns against overstating the significance of AI in elections, which could lead to exaggerated fears and suspicions regarding truth and falsehood.

1 The Expert Group's mandate, composition, and work

1.1 Background for the Expert Group

In the *super election year* of 2024, a historically high proportion of the world's population went to the polls in over 60 countries, including the United States, the United Kingdom, France, India, and Pakistan. The European Parliament election was also held, with voters across all EU Member States casting their votes. The emergence of AI—in particular, the novel opportunities presented by generative AI—has led to growing concerns of adverse impacts on free and democratic elections. This technology alters the landscape of challenges, not only for elections but also for the very foundation of democracies.

Even before 2024, there were examples of disconcerting events. Fake, AI-generated audio recordings garnered significant attention during the 2023 Slovakian election campaign. During the 2023 Norwegian local elections, a fake, parody website for the local electoral list *Sørlandspartiet* was uncovered, where AI had been used to generate images of non-existent candidates.¹ Therefore, at the turn of the year, considerable tension surrounded the potential of AI to create or amplify challenges impacting the election process and related communication in 2024. From 2024, the Expert Group highlights the elections in Romania and the United States as being of particular interest, although several other elections conducted this year are relevant and instructive for Norway. These are discussed in Chapter 4.

Experiences from 2024 provide Norway with a unique opportunity to learn from other countries. Therefore, the Government decided to appoint a fast-working Expert Group to make recommendations on measures that can be implemented to mitigate the adverse impacts of AI for the upcoming Norwegian parliamentary election and the Sámi parliamentary elections in 2025.

At the start of 2024, AI-generated misinformation and disinformation were by many considered to be among the biggest global risks.² In their respective reports, the Norwegian National Security Authority and the Norwegian Police Security Service

¹ Heggheim and Sællmann, 2023

² World Economic Forum, 2024

emphasise the advent of AI as one of the development trends that will impact national security.³

Norway has a well-functioning and stable democratic system that must be safeguarded. Our society is characterised by openness, trust, an educated and digitally literate population, a diversity of editorial media, well-developed infrastructure and a digital public administration. These characteristics foster resilience and serve as a firm foundation for mitigating the adverse impacts of new technology. However, we cannot take these strengths for granted.

The challenges AI presents to elections and democracy extend beyond Norway's national borders. The use of AI raises a number of issues, including changes in the information landscape, ethics, privacy, security, cybersecurity, copyright, infrastructure, national autonomy and human rights. This requires international cooperation and Norwegian engagement on the global stage, alongside comprehensive national assessments and measures.

1.2 Mandate

The Expert Group was given a mandate by the Ministry of Local Government and Regional Development, which is summarised in Box 1.1.

Box 1. 1 Mandate for a fast-working expert group to look at the significance of artificial intelligence (AI) for secure and democratic elections

Background

Generative AI can produce text, audio, images, and video that increasingly resemble authentic content. It is becoming increasingly difficult to distinguish between what has been created by humans and what has been created by AI. AI-based tools are also becoming increasingly widespread, and many people use them as a source of information instead of traditional search engines. Such developments could have a

³ The Norwegian National Security Authority, 2024; The Norwegian Police Security Service, 2024

major impact on how voters receive information about elections and about the various political parties and candidates, and may potentially influence the political debate and agenda.

In 2024, elections will be held in several of the most populous countries in the world, as well as to the European Parliament. The elections held in 2024 will provide new information about the significance of AI for democratic and secure elections, including how AI can be used in influence operations and its significance for information dissemination. This experience will enable us to prepare for upcoming elections in Norway, helping to ensure Norway is equipped to meet the challenges posed by AI in this context.

The Expert Group is tasked with

- Describing how AI is altering the challenges facing democracy, and its potential significance for elections;
- Determining the various ways AI tools can be used to exert unwanted influence;
- Identifying the vulnerabilities arising from the increased prevalence of AI and artificially generated content;
- Gathering experience on how other countries are working to counter election influence; and
- Proposing measures that can be implemented before the 2025 parliamentary election to meet the challenges that AI poses to Norwegian democracy and to ensure confidence in Norwegian elections.

The Expert Group will contribute to

- A better overview of existing knowledge about the use of AI in the context of elections;
- Improve competence on how AI can be used to influence elections; and
- An informed debate about the use of AI in Norway, based on Norwegian conditions.

Nature of the work

The Expert Group will submit a written summary of experience gained from the elections held in 2024. The Expert Group is otherwise at liberty to determine how to present its work, for example in the form of short publications and a seminar, or similar.

The proposed measures should increase resilience to disinformation created by AI, and should be implemented before the 2025 parliamentary election. The measures will be presented to the inter-ministerial working group tasked with strengthening

resilience to undesirable influence in elections, which has been appointed by the Government with a mandate until the 2025 parliamentary election.

The Expert Group aims to present the results of its work by 31 December 2024.⁴

1.2.1 The Expert Group's interpretation of the mandate

The Expert Group has been assigned a broad mandate to be carried out within a limited timeframe. To be able to provide relevant and appropriate advice in time for any measures to be implemented or initiated before the 2025 parliamentary election, the group has had to prioritise which areas to emphasise in its work.

The mandate emphasises that the group should describe how AI is “altering the challenges facing democracy, and its potential significance for elections”. The group understands the mandate to mean that the significance for elections is at the core of the assignment and should be given the greatest emphasis. The mandate is not understood to mean that the Expert Group is to provide a comprehensive overview of AI's potential impact on democracy at large. Therefore, the emphasis is on identifying changes in the challenges and what measures can be implemented to reduce the risk of AI being used in ways that will be detrimental to democracy in general and elections in particular.

One of the main tasks in the assignment is to gather experiences from other countries that held elections in 2024. The Expert Group believes it is important to contextualise the experiences in terms of their relevance to Norwegian elections. Therefore, the Expert Group uses Norwegian conditions as its starting point when discussing which new technological AI breakthroughs might create or reinforce elections. Our recommendations for action will also be aimed at our national context.

The mandate states that important reasons for the work are new or increased threats and vulnerabilities that can be linked to AI, particularly with regard to the risk of unwanted election influence. However, the assignment is not limited to this; it encompasses a broader scope. AI could also have a major impact on the information landscape in Norway, as well as on cybersecurity. In our work, we have therefore chosen to pursue three areas in terms of the impact AI may have on elections in Norway. The main areas are discussed in more detail in Chapter 3.

⁴ After the mandate was established, the deadline for finalisation was postponed to February to ensure sufficient time to assess the material.

Technological developments are advancing rapidly, and the Expert Group finds it necessary to highlight the changes in the landscape of challenges and overarching measures within these three areas that will extend beyond the 2025 election.

1.3 Composition

The Expert Group was appointed by the Ministry of Local Government and Regional Development on 6 June 2024. The Expert Group has consisted of:

- Niels Nagelhus Schia, Senior Research Fellow and Professor at the Norwegian Institute of International Affairs (NUPI), Chair of the Expert Group
- Anne Sofie Molandsveen, Thematic Manager for Democracy and Elections at NORCAP – Norwegian Refugee Council
- Bente Kalsnes, Professor at the Department of Communication, Kristiania University of Applied Sciences
- Heidrun Åm, Professor at the Department for Sociology and Political Science, Norwegian University of Science and Technology (NTNU).
- Helle Sjøvaag, Professor at the Department of Media and Social Sciences, University of Stavanger
- Julie Ane Ødegaard Borge, Associate Professor at the Teachers Education Programme, NLA Bergen University College
- Lars Raaum, Community and Government Relations contact person, Norwegian Media Businesses' Association
- Rune Karlsen, Professor at the Department of Media and Communication, University of Oslo

The Expert Group has received secretariat support from the Ministry of Local Government and Regional Development. The secretariat has consisted of Senior Advisor Sissel Lian (from June to October 2024), Senior Advisor Øyvind Kind Robertsen and Consultant Vilde Sollien (from September 2024).

1.4 The work of the Expert Group

The Expert Group held its first meeting on 12 June 2024. The Expert Group has held a total of seven full-day meetings, as well as several shorter meetings. The group received input from experts and actors in the media sector, the security sector, academia, technology platforms, technology communities, political parties and election authorities. The input has mainly been provided in the form of presentations and dialogue at the Expert Group's meetings and study visits, and in some cases at separate meetings.

In the autumn of 2024, three study visits were made to four different destinations. Study visits were made to Helsinki in September, London, and Brussels in October and

Washington D.C. in November. The purpose of these study visits has been to meet with election authorities, security authorities, research institutions and other relevant actors, and to learn how these countries have worked on this subject prior to, during and following elections.

The Expert Group sent an enquiry, via the Ministry of Foreign Affairs, to Norway's foreign and permanent missions/delegations, requesting information about how the countries they follow have worked with AI and elections, as well as any examples. The Expert Group also asked requested input on whether the embassies and missions/delegations knew of any relevant researchers, organisations or institutions that had in-depth knowledge of this subject.

An overview of who contributed input to the Expert Group can be found in Appendix 1 to this report.

1.5 Key terms

The following is an explanation of key terms used in the report.

Artificial intelligence, abbreviated as AI, is a term that encompasses various technological tools that can be used for different tasks. An Expert Group appointed by the EU defined AI as follows:

AI systems act in the physical or digital dimension by perceiving their environment, processing and interpreting information and deciding the best action(s) to take to achieve the given goal. Some AI systems adapt their behaviour by analysing how the environment is affected by their previous actions.⁵

AI is a tool that can be used in ways that can have both a positive and negative impact on elections and democracy. AI is used to a significant extent in society today. Social media and other technology platforms, for example, make extensive use of AI, partly through the algorithms that determine what content is displayed and spread to users.

AI as such is not a new field, but in recent years, developments in the area of **generative AI** have particularly accelerated. Generative AI is based and trained on large amounts of data and can create content in various formats such as text, audio, image, and film. The content may *appear* original, but the content is created on the basis of the data on which the model has been trained. No specific knowledge is required to be able to use the

⁵ Independent High Level Expert Group on Artificial Intelligence set up by the European Commission, 2018, translation from National Strategy for Artificial Intelligence.

tools for simple purposes, as the user can communicate with the tool using plain speech.

The emergence of generative AI has particularly raised concerns that the technology could have an impact on elections and democracy – whether through deliberate misuse or because the data does not provide an accurate picture. For instance, fabricated images, videos, or audio recordings that are made to look or sound like certain people, known as *deepfakes*, have attracted a great deal of attention. Chatbots based on generative AI have also become widespread.

The fear of technology misuse is particularly associated with the manipulation of information in connection with influence operations or disinformation campaigns, which can be used to disrupt the election process and weaken confidence in its conduct and results. In the following terms, the Expert Group builds on definitions given by the Commission on the Freedom of Expression⁶ and the Norwegian Defence Research Establishment⁷.

Elections – particularly election campaigns – are about influencing voters. It is a legitimate part of democracy, and it is important to ensure that measures to prevent unwanted influence do not simultaneously undermine important democratic principles. **Unwanted election influence** refers to factors that influence individuals' choices or perceptions in a manipulative, unethical, undemocratic or illegal manner, often through the use of disinformation, social manipulation, and technological tools. This violates the individual's right to make informed and free choices and can undermine trust in electoral processes and democratic institutions.

In the public debate, this term is mainly in reference to influence operations by foreign actors, but an influence operation can also be carried out or supported by a domestic actor.

Disinformation, on the other hand, refers to the dissemination of deliberately false or misleading information, where the purpose is to damage or influence the recipients' opinions, attitudes, or actions.

Misinformation is used to describe incorrect information that is disseminated without malicious intent. In other words, the purpose of the dissemination of information is not always clear, and the actor may be unaware of the veracity of what is being shared.

⁶ Official Norwegian Report (NOU) 2022: 9

⁷ Sivertsen, et al., 2021

2 Technology, media, elections, and democracy – the situation in Norway

In this chapter, we will review key frameworks for Norwegian democracy and provide a basis for assessments of security, elections, media landscape, democracy, trust, and infrastructure in a Norwegian context. Furthermore, we will also provide a brief overview of relevant EU legislation. This review is the Expert Group's starting point for assessing how AI could have an impact on elections and democracy in Norway.

2.1 Security policy situation

Intelligence and security services issue annual threat and risk assessments. For several years, these assessments have highlighted foreign influence – particularly from Russian and Chinese actors – as a threat. Elections are important events which threat actors may attempt to exploit by way of targeted influence operations.

In its threat assessment for 2024⁸, the Norwegian National Security Authority (NSM) points out that the results of the 2024 election year could have major impacts on security policy development for democracies worldwide. They point out that threat actors' use of technology can evolve faster than the open democracies' ability to protect themselves. Information technology and complex instruments can be utilised to target democracies with open information environments, such as Norway. NSM also highlights AI and the risk that this technology can be used to undermine and influence democratic elections. They note that AI enables the spread and fabrication of misinformation and disinformation in a way that can challenge the foundations of democracies. At the same time, AI can also be used to distinguish between malicious and legitimate activity, and AI will likely be important for analysing and detecting operations against Norwegian targets.

A number of global and national governments and organisations identified the (mis)use of AI as an important part of the threat landscape in 2024. In January 2024, the World Economic Forum published its Global Risks Report 2024. The report emphasises that AI, which can be misused to spread false and untrue information, poses one of the top global risks in the coming years.⁹ The report from the UN High-Level Panel on Artificial

⁸ The Norwegian National Security Authority, 2024

⁹ World Economic Forum, 2024

Intelligence from September 2024 also points to elections as an area where AI can pose a risk.¹⁰

2.2 The election process in Norway

2.2.1 Roles and responsibilities

The Constitution of Norway includes certain overarching frameworks for how parliamentary elections should be conducted. The Election Act and the associated Election Regulations regulate the implementation of parliamentary, municipal and County council elections. Separate provisions in the Sámi Act and Regulations on Sámi Parliament Elections regulate the conduct of elections to the Sámi Parliament.

The Ministry of Local Government and Regional Development has the overall national responsibility for the conduct of elections in Norway and administers the legislation relating to elections. This also means that the ministry coordinates the work on security and emergency preparedness related to the election process.

The main task of the *Norwegian Directorate of Elections* is to provide municipalities and county authorities with the tools and support that will enable them to conduct elections. They develop and operate the electronic election administration system EVA, which is used by all municipalities and county authorities. The Norwegian Directorate of Elections provides the municipalities with training and user support for the system. Furthermore, they are responsible for governmental information on elections that is provided to the population.

It is the *electoral committee in each municipality* that has the overall responsibility for the practical aspects of conducting elections in Norway. The municipalities decide the time and place for voting and recruit and train election workers. They are responsible for the practical implementation of voting and for the counting and keeping of the protocol for the election. This also means that each municipality is responsible for security and emergency preparedness related to the practical conduct of elections locally. *The county electoral committee* in each county authority is responsible for approving list proposals and counting votes in county council and parliamentary elections.

2.2.2 Use of technology in the election process

The Norwegian Directorate of Elections' services are largely digital. The electronic election administration system EVA is used by all municipalities and county authorities in

¹⁰ United Nations AI Advisory Body, 2024

election preparations, during voting, counting and election returns. The Election Act Commission pointed out that Norway uses technology in its election process to a greater extent than our neighbouring countries. Among other things, the Commission proposed that the use of EVA should be codified in law.¹¹ The Storting adopted the codification of EVA as part of the new Election Act in 2023, cf. Section 20-1 of the Election Act. The new Election Act entered into force in May 2024, and the parliamentary election in 2025 will therefore be the first election conducted under the new Act.

Voters themselves do not use electronic solutions for voting. All voting in Norwegian elections takes place using paper ballots, including advance voting and votes from Norwegians living abroad (advance voting is discussed in more detail under 2.2.4). In the event of technical problems with the system or lack of internet access during the election, which, for example, may prevent access to the electronic electoral register, there are manual contingency procedures.

All ballots shall be counted at least twice. The first count of ballot papers must be done by hand by election workers, while the municipalities can choose to use machine counting that employs scanners in the second count.

In 2011 and 2013, trials of online voting were carried out in selected municipalities. However, these trials were discontinued prior to the 2015 election. Due to a lack of political agreement, the trials were not continued. In later assessments of electronic voting, the security challenges of electronic solutions are particularly emphasised as a problem.¹²

2.2.3 Security efforts in connection with elections

Prior to the municipal and county council elections in 2019, the Government set up an interdepartmental working group with the aim of increasing resilience against unwanted influence in connection with elections.¹³ The working group is chaired by the Ministry of Local Government and Regional Development and consists of relevant government ministries and subordinate agencies, including intelligence and security services. The working group was reappointed before the 2021 and 2023 elections and now has a mandate that extends until the 2025 elections. Ahead of the last elections, the Government has presented an action plan based on the work of the working group, with

¹¹ Official Norwegian Report (NOU) 2020: 6

¹² Oslo Economics and the Norwegian Computing Centre, NR, 2023

¹³ Prop. 45 (Bill) (2022-2023)

measures that will contribute to increased resilience against unwanted influence of elections, and will do the same before the parliamentary election in 2025. The initiatives have been aimed at voters, political parties and candidates, municipalities and election authorities. The measures prior to the municipal and county council elections in 2023 included a cross-sectoral collaborative conference on unwanted election influence, an educational programme to strengthen pupils' critical media literacy and the distribution of an information brochure with good security advice for all candidates standing for election.¹⁴

The Norwegian Directorate of Elections performs a thorough testing of the electronic systems used in the election process. They also provide guidance to the municipalities and publish a security guide to help the municipalities conduct secure elections. The guide provides advice on physical security, organisational and human security measures, and information security related to the use of EVA.

2.2.4 Voting patterns and variations in voter turnout

Norway has a long advance voting period. Ordinary advance voting starts on 10 August and runs until the last Friday before election day, which always falls on a Monday in September.¹⁵

Voters are increasingly opting to vote in advance, resulting in a growing proportion of the actual voting being conducted prior to election day. The municipalities have also largely made it easier to vote in advance. In the 2021 parliamentary election, for the first time, more than half of voters (58 per cent) voted in advance. This was a sharp increase from 2017, when 36 per cent of voters voted in advance. The fact that the election was held during the COVID-19 pandemic probably had an impact on this sharp increase. Nevertheless, the proportion of advance votes remained high in the municipal and county council elections in 2023, when 49 per cent of voters voted in advance.¹⁶

There are variations among those who participate in elections. Through the Norwegian Program of Electoral Research, it has been possible to follow voters over several elections. By doing so, it has been determined that there is a group with just under 10

¹⁴ Ministry of Local Government and Regional Development, 2023a

¹⁵ It is possible to vote as early as 1 July, when early voting opens, by contacting the municipality and requesting to vote, cf. Section 7-1, second paragraph of the Election Act.

¹⁶ Kleven, 2023

per cent of eligible voters who never vote. Persons with low levels of education, young men and voters with immigrant backgrounds are overrepresented among so-called “permanent non-voters”.¹⁷

At the last parliamentary election in 2021, participation was highest in the 60-79 age group, while those with the lowest participation were so-called *second-time voters*, i.e. voters ages 22-25. In the younger age groups, the gender differences are also clear, and among all voters under the age of 30, participation among women is 12 percentage points higher than among men. In this age group, the differences in participation between the genders also increased between 2017 and 2021.¹⁸

2.2.5 Election campaign

Election campaigns in Norway are largely centred around the political parties. Parties often play a more central role than the individual candidates. Voters are interested and follow election campaigns both through editorial media and social media. A majority of voters decide what to vote for during the election campaign, and around one-fourth tend to change their party preference during the campaign.¹⁹ This indicates that election campaigns have an important function for voters’ choice of political party and thus also for election outcomes.

There are no regulations governing how political parties conduct election campaigns in Norway, apart from a ban on advertisements on television for political messages, cf. Section 3-1 of the Broadcasting Act. There is no corresponding ban on other platforms. Nor does Norway have any regulations regarding when political parties can begin or end election campaign activities, as certain other countries do.

Norway offers generous state funding for political parties, which is the largest source of funding for most political parties, including during election campaigns. Government funding is given to all registered political parties that have stood for election and received votes. Political parties are not required to have achieved representation. In addition, parties may receive support from others but are not permitted to accept contributions from donors who are unknown to the party or from foreign donors, cf. Section 17a of the Norwegian Political Parties Act. Contributions above certain thresholds set out in the Political Parties Act are identified and publicised. In election

¹⁷ Bergh, Christensen and Holmås, 2021

¹⁸ Bergh, Christensen and Holmås, 2023

¹⁹ Karlsen, under publication

years, all contributions exceeding NOK 10,000 must be reported as they come in and will be published on the website Partifinansiering.no. Contributions also include non-monetary contributions. The Political Parties Act Committee, which is tasked with interpreting the legislation and monitoring compliance with the rules governing funding in the Act, has noted some weaknesses in the Political Parties Act and suggested that amendments are needed. These weaknesses include the fact that influence can be exerted through indirect contributions from an action group or through support for unregistered parties/lists and their individual candidates (which are not bound by the reporting obligation).²⁰ In other words, the actual contributor may be anonymous to the public, even if the name and value of the contribution is made known, as contributions are channelled through third-party actors.

2.3 Media and technology use in Norway

In recent decades, Norwegians' media consumption has, as a whole, changed rapidly in line with technological developments. The following is a brief review of Norwegians' use of editor-controlled media, social media and the use of technology.

2.3.1 Editor-controlled media and its use

Free, independent and truth-seeking media is a democratic infrastructure that fulfils important tasks in information distribution, debate and social criticism. Editor-controlled media works according to professional journalistic methods based on a code of ethics for the press, with a responsible editor who is accountable for what is published. In Norway, editorial independence is safeguarded through the Rights and Duties of the Editor [Redaktørplakaten] and the Media Liability Act. Norwegian editor-controlled media have undertaken to comply with the Code of Ethics of the Norwegian Press, and media affiliated with the Norwegian Press Association can lodge complaints with the self-regulatory organisation, the Norwegian Press Complaints Commission.

Media regulation supports media diversity through instruments such as direct press subsidies, VAT exemptions and support for public broadcasting, which are intended to secure media throughout the country, ensure competition and safeguard daily news and diverse interests. Media diversity is thus intended to both support the principle of representation in democracy and prevent groups from feeling that they are not reflected in society's political processes.

²⁰ The Political Parties Act Committee, 2023

News consumption among Norwegians is characterised by a stable and high level of trust in editor-controlled journalistic media. According to the Norwegian Media Authority, 73 per cent of the population have fairly high or very high trust in Norwegian news media in general.²¹ In the 2024 Norwegian Citizen Survey [Innbyggerundersøkelsen], conducted by the Norwegian Agency for Public and Financial Management (DFØ), the population was asked about their media habits. Eight out of ten responded that they *usually* use editorial media such as newspapers and online newspapers as a source of news and politics, seven out of ten use TV as a source, and four out of ten use radio.²² However, some groups in society, such as young people and immigrants, use editor-controlled media significantly less than others. In recent years, there has been a decline in the use of editor-controlled media platforms among younger users, but an increase in the use of social media.

Compared to many other countries, Norwegians have a strong willingness to pay for online newspapers and news applications, in fact the highest in the world, according to Reuters News Report.²³ Norwegians are also far more likely to go directly to the source to the media's own websites and apps, and are less likely to use social media and search engines as sources of news.²⁴

The Norwegian Media Authority points out that Norwegian media find themselves in a more economically uncertain period, and that newspaper profitability is at its lowest level since the financial crisis of 2022 and 2023. The role of editorial media in society is also under increasing pressure from global platforms, both in terms of usage and revenue.²⁵

2.3.2 Social media and its use

Social media does not have editors curating its content, but is instead driven by algorithms that control what users see. The types of content users are exposed to is based on the social media's recommendation system and the companies' business models.

²¹ The Norwegian Media Authority, 2023

²² The Norwegian Agency for Public and Financial Management (DFØ), 2024

²³ Newman, Fletcher, Robertson, Arguedas and Nielsen, 2024

²⁴ Olsen, Kalsnes and Barland, 2024

²⁵ The Norwegian Media Authority, 2024a

One challenge with social media, which has been highlighted by the Total Defence Commission, among others, is that it contributes to changing how people communicate, share information and interact with one another. Due to social media algorithms, users may largely only be exposed to content or like-minded people, which would help confirm and reinforce their existing perceptions and spare them from content that might help to challenge their perceptions. This could lead to increased polarisation and undermine trust in society.²⁶

The way that many social media platforms work has changed over time. From being based on friendships that users actively confirmed themselves, the platforms are now increasingly being driven by AI and algorithms. In addition, they have gone from being text-based to focusing more on images and videos.

In recent years, there has been a growing fragmentation internationally in the use of social media. The choice of which social media to use, may be associated with age, but also with political views.²⁷ In Norway, the choice of social media is to a lesser extent based on political views, but there are major generational differences in the use of social media. Facebook/Messenger is the largest social media platform in Norway, and in 2023, 63 per cent reported using Facebook during an average day. This was followed by Snapchat (56 per cent), Instagram (46 per cent) and TikTok (22 per cent). However, there are significant variations in usage between different age groups, and TikTok and Snapchat in particular stand out as having by far the highest usage among the youngest age groups.²⁸ Internationally, *hybrid apps* such as WhatsApp and Telegram are growing. These are primarily viewed as platforms for messaging. However, groups can have a large number of followers, even millions in some cases. These platforms currently play a much smaller role in Norway than in other parts of the world.

As a source of news, social media has become increasingly common. In 2023, 57 per cent of the population stated that they find and read news on social media on an average day. 79 per cent of young people between the ages of 16 and 24 consume news through social media. A significant proportion of older age groups also find and read news on social media.²⁹

²⁶ Official Norwegian Report (NOU) 2023: 17

²⁷ Muñoz, 2024

²⁸ Bekkengen, 2024

²⁹ Ibid.

In social media, it is difficult to distinguish between different senders, and the platforms usually present content from editor-controlled media in the same manner as advertising and content from influencers. Most media organisations are present on the largest social media platforms to share their information and try to attract readers to their pages. Over time, however, there has been a trend in social media, including Facebook, towards de-prioritising content from editor-controlled media, in favour of other content that could create more engagement.^{30,31} This has led to an increasing number of influencers. In its report for 2024, the Reuters Institute points to the emergence of news profiles that may have a greater reach than editor-controlled media and their profiles, especially in the United States.³²

2.3.3 Norwegians' familiarity with, and use of AI

Statistics Norway (SSB) has studied Norwegian households' general use of ICT, including AI. At the beginning of 2024, Statistics Norway found that the use of AI varied in terms of gender, age and county. Overall, a higher number of men than women use AI, with 42 per cent men and 30 per cent women. The exception is women aged 16-24, where 68 per cent of women use AI compared to 62 per cent of men.³³

Furthermore, Statistics Norway found that 65 per cent of Norwegians between the ages of 16 and 24 have used generative AI. Usage decreases thereafter with age: 53 per cent of people ages between 25 and 34, and 9-10 per cent of those over 65. 64 per cent of the population do not use generative AI. The vast majority of these state that they have no need for it. Others say they do not know how to use the technology, are worried about privacy, or did not realise that such tools existed.

The Centre for Research on Civil Society and the Voluntary Sector has also studied Norwegians' use of AI and found that familiarity with AI and the use of AI tools is widespread, but that trust in AI is low. This low level of trust is primarily due to societal consequences related to both "problematic use" and "unintended consequences". This distinguishes itself from the positive effects, such as AI contributing to increased

³⁰ Wong, 2018

³¹ Jerijervi and Hauger, 2023

³² Newman, Fletcher, Robertson, Arguedas and Nielsen, 2024

³³ Rybalka, 2024

productivity and efficiency, which is beneficial to society, but can also affect unemployment.³⁴

They also find clear correlations in the use, attitudes, and knowledge of AI between different socio-economic groups. Norwegians with higher education are more likely to use AI, have fewer concerns about the consequences for their working lives and are positive about the opportunities AI offers. This group's main concerns appear to be broader societal consequences, such as political manipulation and increased power for technology companies. The largest user group of AI includes young (under 45 years of age), educated men with high incomes (over NOK 700,000). Women over the age of 45 with a lower level of education and income are less likely to use AI. This group faces more user challenges, is more worried about negative consequences, and has less faith in positive effects, both in their work and leisure time. Just as there are differences in the use of IT tools, there may be a similar distinction between those who do and do not use AI. Norwegians use AI tools mainly for work involving writing and texts, but also for entertainment, teaching and inspiration.³⁵

Reuters News Report finds that 37 per cent of Norwegians say they have heard of AI or read quite a lot or a great deal about AI. Compared to other countries, Norway is below the average, which is 45 per cent. Thus, they conclude that Norwegians do not appear to be very knowledgeable about AI.³⁶

The Norwegian Media Authority has conducted a survey of critical media literacy in the Norwegian population.³⁷ Here, they mention how technological development – and particularly the emergence of generative AI – has reinforced the distinction between reliable and unreliable sources of information. Their report shows that there are major differences in people's belief in their own ability to distinguish AI-generated content from non-AI generated content.

Many of the respondents in this survey used AI services to find information (53 per cent) and to get help with writing (45 per cent). Some also sought out such tools out of curiosity to see how AI works (41 per cent). Among those who have used AI services, it appears that 40 per cent have considered the information to be correct and credible to a

³⁴ Solheim and Enjolras, 2023

³⁵ Ibid.

³⁶ Moe and Bjørgan, 2024

³⁷ The Norwegian Media Authority, 2024b

very large or large extent, compared to 13 per cent who have considered the information to be correct or credible to a small or very small extent. At the same time, there are significant differences between younger and older target groups in terms of their confidence about the truth value of AI-generated content. The younger share of the population uses AI the most and has the greatest confidence that the information is accurate and credible. Many in this group also find it easy to assess whether the information they find online is true or false.³⁸ Older age groups are more concerned that AI is making it more difficult to distinguish true information from false information online. Among those over age 35, 81 per cent are either very worried or somewhat worried, compared to 62 per cent of younger people. This may be related to the fact that older age groups are less familiar with new digital tools, use AI services to a lesser extent, and have greater concerns about AI.³⁹

There are also signs that AI tools are becoming more important as a source of information. Kantar's survey of media trends among young people indicates that the use of traditional search engines such as Google is declining among young people, and that many in this age group prefer services such as ChatGPT, as well as TikTok, as sources of information.⁴⁰

2.3.4 The role of media in election campaigns

Editor-controlled media plays a key role in democracy, particularly in connection with elections, by being a credible and quality-assured source of information for the population and by conducting critical journalism and providing an arena for debate. Election research has shown that Norwegians are major consumers of news from editor-controlled media during election campaigns, and that the proportion of people who receive daily news about the election increases in the run-up to election day, even among the least politically interested.⁴¹ In the parliamentary election survey for the 2021 parliamentary election, it was found that most voters had read, seen or heard news about politics and societal issues from NRK TV. Local newspapers and radio also reach many people. The use of Facebook as a news source remained stable from the 2017

³⁸ Ibid.

³⁹ Ibid.

⁴⁰ Hofsrud, 2024

⁴¹ Haugsgjerd and Karlsen, 2022

parliamentary election to 2021, with around 20 per cent stating that they used it as a source of daily news.⁴²

Local election surveys conducted in connection with each municipal and county council election also show that voters use local, regional and national media to acquire news about the election. At the same time, there are certain differences between groups in society. The use of editor-controlled media increases the higher the voter's education, while there is no similar effect for the use of social media. In 2019, it was found that social media is more important for younger people and for women than for other groups.⁴³

2.4 Democracy and trust

Norway is a solid, well-functioning and stable democracy. This is underpinned by the fact that Norway has long been at the top of various global democracy surveys, such as The Economist Democracy Index⁴⁴ and Varieties of Democracy⁴⁵.

The Report on the status of Norwegian Democracy, conducted by researchers at the University of Oslo, also concludes that Norway is one of the world's most democratic countries. Norwegian democracy generally holds a high standard across the various dimensions analysed, but there is also room for improvement.⁴⁶ Researchers behind the Report on the status of Norwegian Democracy surveyed more than 100 experts on Norwegian politics and democracy. They find that Norwegian democracy *is probably* quite resilient in the face of what is referred to as "authoritarian challenges". However, this does not mean that Norwegian democracy is immune to democratic decline. Among the challenges highlighted in the survey is that citizens believe there to be a widespread abuse of power and corruption. The Norwegian Citizen Survey [Innbyggerundersøkelsen], conducted by the Norwegian Agency for Public and Financial Management (DFØ), also reveals a decline in confidence that parliamentary politicians work for the good of the people, as well as an increase in the proportion responding

⁴² Haugsgjerd, Karlsen and Aalberg, 2023; Kalsnes and Ihlebæk, 2021

⁴³ Karlsen and Steen-Johansen, 2021

⁴⁴ Economist Intelligence, 2024

⁴⁵ V-Dem Institute, 2024

⁴⁶ Knutsen et al., 2023

that they believe corruption occurs in the central government and in municipalities.⁴⁷ Another area noted by the Report on the status of Norwegian Democracy is an apparent increase in threats towards and harassment of politicians. As a consequence, politicians may self-censor themselves by declining to participate in debates on certain topics or by withdrawing from politics. A skewed distribution of political influence is also noted at the group level.

The high level of trust has been cited as a factor in explaining why Norwegian democracy is strong. By international standards, Norwegians have a high level of trust in one another and in the media, the authorities and political actors at both the national and local levels. However, trust is not evenly distributed in society. In one study on trust in local politics, researchers found that groups that can be considered “politically resourceful”, basically middle-aged, working people with a higher education, tend to have the highest trust in local political actors and institutions. The same study also found that there was a greater decline in trust in the groups that initially had lower political trust, which may indicate increasing differences in trust.⁴⁸ There are also differences with respect to confidence in elections themselves, particularly between those who vote and those who do not. In the 2023 Election Survey, voters were asked whether they trusted that the election had been conducted correctly, and could answer on a scale from 0 to 10, where 10 meant that the voter fully trusted that the election had been conducted correctly. The survey found that more than half of those who voted in 2023 responded that they had full confidence that the election had been conducted correctly, i.e. they responded with the highest possible score. Although the majority of those who did not vote also answered that they had confidence, 17 per cent of these placed themselves in the middle category, compared to 6 per cent of the group who did vote.⁴⁹

Although Norwegian democracy is considered fairly resistant to authoritarian forces, there are nevertheless certain trends that highlight vulnerabilities in this area. Surveys conducted among Norwegian grade 9 pupils have shown that Norwegian pupils are less likely to recognise threats to democracy when presented with them, than pupils in corresponding grades in Sweden and Denmark.⁵⁰ In an as yet unpublished study cited in

⁴⁷ The Norwegian Agency for Public and Financial Management (DFØ), 2024

⁴⁸ Haugsgjerd and Seggaard, 2020

⁴⁹ Kleven and Bergseteren, 2024

⁵⁰ Caspersen, Wendelborg and Storstad, 2023

an article in the newspaper VG, Norwegian researchers noted that undemocratic conduct by politicians is punished by Norwegian voters, but to a lesser extent than one might have hoped. In other words, attitudes to specific issues are given greater weight than whether candidates conduct themselves in accordance with democratic principles. The propensity to tolerate undemocratic conduct by politicians appears to be highest in the youngest voter group (ages 18-29).⁵¹

Freedom of expression is a prerequisite for democracy. In 2022, the Norwegian Commission for Freedom of Expression determined that freedom of expression is strong in Norway. They also concluded that the internet has strengthened the freedom of expression. Nevertheless, they mentioned a number of challenges, including a digital public sphere controlled by global technology platforms and an increasing risk of misinformation and disinformation.⁵² The Norwegian Human Rights Institution and the Norwegian Board of Technology have in furthermore pointed out that the emergence of generative AI reinforces the Norwegian Commission for Freedom of Expression's analysis of the negative effects of the new digital public sphere.⁵³

2.5 Norway's digital infrastructure

The digital infrastructure in Norway consists of a foundation of functions that ensure the distribution of information. Behind social media and other applications and platforms that provide access to content, there is a physical layer consisting of cables, servers, and hubs that are managed by algorithms and other protocols for data traffic. Fibre optic cables that lead under water and over land connect Norway to the rest of the world and enable communication between different parts of the country.

The resilience of these infrastructure value chains is essential for maintaining a robust communications infrastructure. Currently, Norway has relatively good redundancy and transparency in its cable and hub infrastructure through public ownership, but around half of the fibre infrastructure in Norway is owned by foreign actors. Intermediate storage networks and cloud services are almost entirely dominated by US technology

⁵¹ Dahlum, Langsæther and Wig, 2024

⁵² Official Norwegian Report (NOU) 2022: 9

⁵³ The Norwegian Human Rights Institution and the Norwegian Board of Technology, 2023

companies.⁵⁴ The data centre industry is growing rapidly, and in recent years, several Norwegian actors have been acquired by foreign investment companies.

Several of the actors in this basic structure also operate at the platform level, such as Google and Meta. The power of the digital infrastructure lies with US technology companies. The physical and platform infrastructure is crucial for distributing information and for the population's ability to communicate, seek information and participate in democracy.

AI plays an important role in the way that data is managed within the digital infrastructure. Cloud services and storage networks move data around their global networks based on automated analyses of price, traffic, and capacity. More than half of ordinary communications data such as searches, emails, and website visits cross borders and leave Norway.⁵⁵ Once data crosses international borders, this triggers digital surveillance. Data protocols that manage the flow of data in the digital infrastructure are therefore an expression of how AI, beyond generative AI, helps shape the flow of information in society and thus have consequences for democracy.

2.6 Legislation and regulation of AI

We do not currently have a specific AI Act in Norway, although there is existing legislation that can contribute to setting certain limits for AI. EU legislation that is also relevant for EEA will also be implemented in Norway and become enshrined in Norwegian law. There are also other international agreements and initiatives, e.g. through the Council of Europe and the OECD. This is an ever-changing landscape with significant ongoing legislative efforts. In the following, we will discuss important EU legislation.

Digital Services Act (DSA)

The DSA will help strengthen the internal market by modernising and clarifying the obligations of online platforms when removing illegal content, and it addresses new issues that have emerged in connection with the platform economy. The Act will thus replace current practices whereby platform owners themselves determine tolerable content. These rules will provide greater democratic control and oversight of the platforms, and reduce the risk of manipulation and illegal content, where the goal is to

⁵⁴ Sjøvaag, Ferrer-Conill and Olsen, 2024; Sjøvaag, Olsen and Ferrer-Conill, 2024

⁵⁵ Gundersen, 2019

ensure a safer internet for consumers, with more open, transparent and trustworthy platforms.⁵⁶

DSA does not regulate what constitutes lawful and unlawful speech. This is done through the legislation of member states, and misinformation and disinformation are protected by the freedom of expression.

The Commission is authorised, through the DSA, to supervise very large online platforms (VLOP) or very large online search engines (VLOSE). This applies to companies that reach more than 10 per cent of the EU population. There is an annual minimum requirement for VLOPs and VLOSEs to conduct an independent audit, and to identify, analyse, and assess risks associated with platform use. The latter requirement entails, among other things, a risk assessment focusing on the risk to the public debate and election processes. In addition, there must be supervision by a national coordinator and appointed supervisors, and transparency reports must be shared.

The national coordinators and the Commission will work together through the European Board for Digital Services (EBDS), acting as an advisory body. In 2024, EBDS chose to prioritise measures against the unwanted influence in elections.⁵⁷

The Code of Practice on Disinformation

The Code of Practice on Disinformation is a tool provided by the European Commission, established in 2018 and revised in 2022. The 44 signatories have committed to limiting disinformation by supporting commitments and taking actions of relevance to their areas of operation. Signatories include actors involved in platform services, advertising, fact-checking, civil society, research, and others.⁵⁸

The EU Artificial Intelligence Act (AI Act)

The AI Act is a legal framework for the regulation of AI. It entered into force on 1 August 2024 and will be implemented over a period of 24 months. Through the EEA Agreement, the AI Act will be enshrined in Norwegian law. It will therefore provide guidelines for

⁵⁶ EØS-notatbasen [EEA Note Database], 2024a

⁵⁷ The Norwegian Media Authority, 2024c

⁵⁸ European Commission, 2022

how Norway should be supervising AI.⁵⁹ The background for the legislation is to ensure safe, reliable and human-centred AI.⁶⁰

The AI Act is based on different applications of AI technologies, categorised into risk categories. This means that the higher the risk posed by the use of AI, the more strictly its use should be regulated.⁶¹ Some applications of AI are *prohibited*, such as influence techniques to manipulate people's subconscious and behaviour, systems that exploit human vulnerability related to age or physical or mental disabilities, systems used by governments to evaluate or classify people's trustworthiness and, with certain exceptions, the use of identification systems in public places that utilise biometric identity markers. Applications of AI in the *high risk* category must be regulated with requirements related to risk management, data management, technical documentation, human supervision and more. In addition, there is a *transparency requirement* that involves the labelling of AI-generated content such as deepfakes and manipulated images.

The AI Act applies to:

- Suppliers that deliver AI tools or market AI tools or basic models.
- Users of AI tools established or located in the EU.
- Suppliers and users outside the EU, if their AI tools are used within the EU.
- Importers and distributors of AI tools.
- Product manufacturers that integrate AI tools in/with their products under their own name or brand.
- Authorised representatives in the EU for suppliers not established in the EU.
- Individuals in the EU affected by these AI tools.⁶²

The European Media Freedom Act

EMFA by the European Parliament and the European Council was adopted on 11 April 2024 and entered into force on 7 May 2024. The Act will be implemented in Norwegian law through the EEA Agreement. Among other things, EMFA aims to ensure media pluralism and independence, and it sets requirements for providers, actors, and

⁵⁹ Baste, Schultz and Osberg, 2023

⁶⁰ Ministry of Digitalisation and Public Governance, 2021

⁶¹ Ibid.

⁶² The Norwegian Digitalisation Agency, n.d.

member states operating in the media market. For example, the Act includes requirements for editorial independence, protection of journalistic sources, editorial independence for public service broadcasters and transparency of ownership in media companies. It also contains provisions to protect editor-controlled media from the unauthorised removal of content on the major online platforms. A technical and practical advisory body will also be established to strengthen cooperation between regulatory authorities in the media field.⁶³

⁶³ EØS-notatbasen [EEA Note Database], 2024b

3 What impact could AI have on elections?

The Expert Group adopts a broad understanding of elections that encompasses more than the practical conduct of elections, and includes the election campaign and the post-election period when the election results are published and discussed.

In its work, the Expert Group has followed three main areas where we believe AI may have an impact on elections and democracy. In these areas, we believe there is particular cause to be vigilant and prepared to avoid negative consequences for elections and democracy:

- The information and media landscape
- Covert election influence
- The election process and cybersecurity

The primary areas are inspired by the tripartite approach used by The Alan Turing Institute in its reports AI-enabled influence on elections, which recognises that AI can be used to influence individuals, pollute the information landscape and affect the conduct and infrastructure of elections. ⁶⁴

These primary areas are not entirely separate and should be viewed in context. For example, an influence operation may also include cyberattacks or be aimed at amplifying conflicts or changing how the information landscape functions

We summarise the main areas and their potential impact in Table 3.1.

⁶⁴ Stockwell, Hughes, Swatton and Bishop, 2024

Table 3.1 The main areas used by the Expert Group as a starting point and examples of changes and significance

Areas where AI may be of importance	Examples of changes	What is its significance
The information and media landscape	<ul style="list-style-type: none"> - AI-generated texts, images, video and audio - AI misinformation and bias - Increased fragmentation of the media landscape - More difficult to distinguish truth from falsehood 	<ul style="list-style-type: none"> - Voting - Trust in information channels - Trust that others are informed - Access to credible information - Dependence on technology companies - Public dialogue
Covert election influence	<ul style="list-style-type: none"> - Amplification of disinformation and manipulation - A growing number of threat actors 	<ul style="list-style-type: none"> - Trust in political institutions and elections - Attitudes and emotions - Voting
The election process and cybersecurity	<ul style="list-style-type: none"> - Increase in the possibility of cyber-attacks and sabotage 	<ul style="list-style-type: none"> - The election process - Confidence in the electoral system, the conduct of elections and election results

3.1 The information and media landscape

A well-functioning information and media landscape with strong editor-controlled media ensures that voters receive quality-assured and credible information and that there is a critical spotlight on issues, parties and candidates, as well as a fact-based public debate that provides voters with an informed basis for casting their vote. A diverse media landscape contributes to broad inclusion and representation of different views.

The information and media landscape has already undergone major changes due to both technological developments that have moved content and readers from paper to the web and new formats, and the fact that social media have become more important news platforms. This has positive aspects, as it provides people with greater access to information and networks. However, it also has negative aspects, such as an increasing fragmentation of the public discourse and an increased concentration of power among some large international platform and technology companies and individuals, such as X-owner Elon Musk, other owners and influencers.

“Traditional” AI, in the form of algorithms, has long been a fundamental part of how social media works. This has contributed to changes in the information landscape by enabling individual users to receive search results, news, and content based on their own interests and interests of similar users. Algorithm-driven logic can also result in greater exposure to misinformation and disinformation.

Generative AI reinforces all these tendencies. Such tools contribute to new ways of producing, distributing, systematising and analysing information, and can lead to changes in where and how voters acquire information.

Generated content can appear in a variety of formats, such as text, audio, images and video, making it possible to produce realistic but still fake content more efficiently and with fewer resources. Much of the use will be unproblematic, although some may have the potential to confuse and mislead while still remaining within the bounds of freedom of expression. Artificially generated misinformation can become so widespread that it undermines confidence in information in general, thereby contributing to the displacement of credible information. This type of content can, for example, be used to mislead or confuse voters about issues and the election process, undermine political opponents, enhance the emotional engagement of voters, or to generate texts for social media and websites. Like other misinformation and disinformation, such content is primarily spread through social platforms.

The big breakthrough for generative AI arrived with chatbots, particularly ChatGPT in November 2022. Since then, other companies have released their own chatbots. Although the most commonly used chatbots are the general bots used by major companies, there are also more specialised variants that have been trained on limited material to answer questions on a specific topic. Since chatbots provide quick and customised answers, many users choose to use these tools to find information instead of traditional search engines.⁶⁵ This shift could be problematic if the language models generate incorrect information about elections, candidates and parties, known as AI hallucinations. Language models can also have intentional or unintentional political biases that are not known to the user, due to the data the model has been trained on. The use of chatbots as a source of information means that the information can be increasingly personalised. The information provided will vary and may not necessarily be available to the general public. Search engines have also begun to include AI-generated

⁶⁵ Skjuve, Brandtzaeg and Følstad, 2024

summaries in search results, such as Google's AI Overview. This gives users an AI-generated response instead of referring them to sources.

Chatbots, bot avatars and similar AI-driven services can make a positive contribution to the dissemination of relevant information, particularly through multilingual accessibility and the universal design of documents for users with visual and hearing impairments. However, such technology can present challenges for electoral authorities at both the local and national levels, as they are tasked with ensuring that voters are correctly informed. There are several examples of chatbots providing incorrect information about elections, which we will return to in Chapters 4 and 5.

AI has already had an impact on the media landscape, both in terms of how editor-run media work and their role in society. The media have actively used AI in certain areas, such as for summaries and in their internal work on research, transcriptions, translations, and text structure. At the same time, the increased prevalence of AI-generated content also means that the media must be more vigilant to avoid being deceived by such content, and they must use more resources to verify content to prevent the publication of inaccurate information. Several have also tried more experimental uses of AI to engage users in new ways. In connection with the US presidential election, for example, the Norwegian newspaper VG had an election chat, and the television station TV 2 had an AI avatar where users could ask questions and get answers from what appeared to be news anchor Kjetil H. Dale. Editor-controlled media's use of AI is based on press ethics, where the editor is the guarantor of the content's credibility. Norwegian editor-controlled media display a high level of awareness and openness about its use of AI and have guidelines in place for AI use.

The media in Norway are given a special framework to support the freedom of expression and public discourse, thus acting as a counterweight to the potential negative effects these developments may have on the election process in Norway. The tools used to safeguard editorially controlled media in the face of disinformation, influence operations and the disappearance of younger users should reflect these changes and aim to strengthen the ability of editorially controlled media to compete and innovate in technological developments.

The potential consequences of AI-based deepfakes, misinformation, and chatbots are serious. It makes it more difficult to distinguish between real and fake content, which undermines trust in the information landscape.⁶⁶ These changes mean that fewer

⁶⁶ Stockwell, Hughes, Swatton and Bishop, 2024

people are exposed to the same content and information, resulting in a more confusing information and media landscape. Overall, the changes discussed above show that the consequences not only have the potential to affect the election process, but the democratic system as a whole.

3.2 Covert election influence

AI can create new opportunities for influencing and manipulating both individuals and groups in society. This applies both to the political influence that is a natural part of an election campaign, but also to covert influence, which is the second main area the Expert Group has studied. See section 1.5 for the Expert Group's definitions of unwanted influence.

Accessible and affordable AI tools can lower the bar for conducting influence operations. Not only can it amplify the power of established threat actors, but it can also lead to new and additional threat actors entering the field. These may include both foreign state and non-state actors and might even open up for attempts at covert election interference from Norwegian actors operating alone or in collaboration with other actors. One example of foreign actors working together in this manner with domestic actors was the dramatic presidential election in Romania held in December 2024, which is discussed in more detail in section 4.1. The Expert Group emphasises that there is a clear principle distinction in between how to counter foreign actors as opposed to domestic actors. Measures and initiatives must not be permitted to restrict Norwegian citizens' freedom of expression.

Covert election influence is not limited to individual events surrounding election day. As the European External Action Service (EEAS) has pointed out, a coordinated influence operation will often take place over a longer period, from long before the election to after it has taken place, and it will have different phases with different intensities of activity.⁶⁷ The Alan Turing Institute notes that there are different stages of an election process and that threat actors have different objectives for their influence at the different stages:⁶⁸

- Before voting begins: The focus of influence operations is on undermining the reputation of specific candidates or swaying voters' views on particular issues.

⁶⁷ EEAS, 2024

⁶⁸ Stockwell, Hughes, Swatton and Bishop, 2024

- During the voting period: The focus is on disrupting and overloading the information space and causing voters confusion on particular issues related to the campaign or election.
- After the election: The focus is on undermining confidence in the election results, for example by creating the impression of electoral fraud, which in turn can lead to a more long-term decline in confidence in the democratic processes.

The Expert Group will emphasise three ways in which AI can be used that may pose particular threats in this context:

1. *Fake users and websites*: Threat actors can use AI to generate various forms of misleading content more effectively than before. Reducing linguistic and, to some extent, cultural barriers. Operating bots and botnets more efficiently. Create and manage fake profiles and fake websites more quickly. There are a number of examples where threat actors have used AI tools to create fake websites that either mimic editor-controlled media with high credibility or pretend to be new online newspapers or websites for (non-existent) research institutes or similar.⁶⁹ These sites are used to disseminate content where the intent is to exert influence by spreading narratives that the threat actor believes will be of benefit through channels that are intended to appear credible and authentic (see Box 3.1 for a discussion of the *Doppelganger* operation). This can potentially make it harder to detect inauthentic behaviour on social media, as it is less resource-intensive to vary both the language and expression. With AI, activities of this type can also automate the creation and content production of such fake users and websites.

⁶⁹ OpenAI, 2024

2. *Increased personalisation:* A threat actor may use AI as part of an influence operation to influence voter attitudes, opinions, and perceptions. This may include the spread of different types of AI-generated disinformation that is more or less tailored to different groups. By targeting content, it is also possible to tailor messages to the recipient based on, for instance, characteristics such as age, gender, place of residence and other personal aspects based on data the actor has access to. By utilising such opportunities, threat actors can target voters more precisely in order to, e.g. convince them to vote differently than they otherwise would, or to abstain from voting. The same techniques can be used more broadly to influence the agenda and debate surrounding an election to highlight particular issues, such as those that may be particularly polarising or that can contribute to reducing trust in society.

3. *Content overflow:* A threat actor can also take advantage of the opportunities provided by AI to create an overflow of AI-generated content, which may include fake news, manipulated videos, manipulated voices and other forms of disinformation. If such disinformation floods various platforms and websites, this could result in a general distrust of the news and other available information. Even more serious is the risk that citizens will no longer trust that others in society are sufficiently informed. Trust in other citizens to make informed choices is crucial to a functioning democracy, but in an information landscape characterised by disinformation, such trust can deteriorate.

Box 3.1 The Doppelganger operation

The Doppelganger operation is an illustrative example of how Russian influence networks function. This operation has targeted many countries since 2022, with a particular focus on undermining support for Ukraine and contributing to division within countries that support Ukraine. A key part of the operation has been to create fake websites. These websites have, among other things, been clones of recognised media and government websites, and they have created websites that promote anti-Ukrainian and pro-Russian content.

Source: EU DisinfoLab, 2024

3.3 The election process and cybersecurity

The third main area used by the Expert Group as a starting point involves the significance of AI for the election process itself and for cybersecurity in connection with elections. Election security has been given increasing attention, and there are a variety of ways in which AI can play a role in this work as well. Threat actors or malicious actors can use AI to carry out destructive activities more quickly, on a larger scale and with fewer resources.

For instance, AI can be used to compromise and manipulate electronic systems used in elections or create chaos through cyberattacks or cyber operations. This may hinder or disrupt the election process itself and create uncertainty about the election results. Such incidents can have an impact in terms of weakened confidence in the integrity of elections and the legitimacy of democratic processes, regardless of whether the attacks actually succeed in inflicting actual harm or making changes to systems.

One example is phishing campaigns, where actors may attempt to defraud or gain access to systems or information, typically by trying to get individuals, such as people associated with election authorities or politicians, to provide information or get them to open links. Using AI tools such as language modelling and voice cloning, threat actors can carry out targeted cyber operations who appear more trustworthy against individuals. AI tools can also be used in large-scale campaigns aimed at disrupting voting, such as through distributed denial-of-service attacks (DDoS), malware placements, automated phone calls or by making election threats.

AI also provides new tools that can be used for programming and reviewing code. There are clear opportunities here to utilise such tools to facilitate and streamline work on the

development of electronic solutions. Code reviews can be useful for uncovering vulnerabilities in electronic solutions, and the European External Action Service has pointed out that “[t]he explosive growth and availability of AI tools may even hold more benefits for defenders than attackers”.⁷⁰ Yet there is also a potential for abuse. The Norwegian National Security Authority (NSM) notes that threat actors are conducting more thorough reconnaissance attacks to learn how to extract the information they are after, and that new tools make it possible for threat actors with less technical expertise to penetrate systems that should be protected.

⁷⁰ EEAS, 2024

4 Lessons learnt from elections conducted in 2024

A key part of the Expert Group's mandate has been to map the experiences of other countries that conducted elections in 2024. This mapping includes what the countries have done in advance of the election to prepare for the possibility that AI would be used in an unwanted fashion, whether there have been incidents in connection with the election that involved the use of AI and how these incidents were managed, as well as whether AI was believed to have had any impact on the conduct or outcome of the election.

The mapping is based on information gathered in three different ways. Firstly, through the study visits the Expert Group made to Finland, the United Kingdom, Belgium and the United States. Secondly, information was based on input from Norwegian foreign missions. In August, all embassies and permanent missions/delegations received a request from the Ministry of Foreign Affairs on behalf of the Expert Group, asking them to provide information about AI and elections in their respective countries. The foreign missions that sent briefings are listed in Appendix 1. Thirdly, the survey is based on public reports from research institutions, technology companies and think tanks, as well as media reports.

The Expert Group has placed particular emphasis on the major elections in Europe and the United States in 2024, as these are elections that are held in countries with long-held democratic traditions where the experiences may be more relevant in a Norwegian context. The following chapter therefore summarises key elections investigated by the Expert Group, as well as certain interesting findings and examples from other countries. Near the end of the Expert Group's work period, elections were held in Romania, which would prove to be the most dramatic example in 2024. Only elections held in 2024 are discussed here, so the much-discussed election in Slovakia is not mentioned here, nor will we discuss the elections in Argentina or Nigeria, as these were all held in 2023.

The Expert Group adds that there could be other incidents that were not identified in this mapping, and we do not intend to describe all incidents in connection with elections where AI has played a role. The focus of the following chapter is to highlight some experiences from different countries and how they have approached this new challenge, and to present a few illustrative examples.

In February 2024, a number of technology companies, in their preparation for the 2024 election year, joined forces in an agreement to combat fake news and track down AI-

generated political content. This initiative is known as the Munich Tech Accord.⁷¹ Through this agreement, companies including Microsoft, Google, Meta, TikTok, Snap, OpenAI, and X, among others, signed on to work to prevent harmful AI-generated content that could mislead voters.

4.1 Romania

The first round of the Romanian presidential election was held on 24 November, but the election results were annulled shortly before the second round was due to be held.⁷² The annulment followed accusations of widespread foreign influence, which allegedly originated in Russia. Russia has denied conducting influence operations targeting the Romanian election.⁷³ This influence is said to have been done through the promotion of Russian-friendly candidates who are sceptical of NATO. The fact that the campaign, shortly before the election, contributed to the extreme, rather unknown presidential candidate Călin Georgescu who suddenly emerged as the winner of the first round of voting drew a great deal of attention.

Much is still unknown about the events in Romania, including the use and scope of AI. The Expert Group believes this election stands out as the most dramatic example from 2024, with allegations of influence operations that combined cyberattacks, social media disinformation and the exploitation of algorithms to maximise spread. The events during the Romanian election illustrate how the three main areas identified by the Expert Group in Chapter 3, information and media landscape, covert election interference and cybersecurity, can interact to amplify threats to democratic elections.

Georgescu's campaign gained momentum on TikTok just before the first round of voting. According to the Digital Forensic Research Lab (DFRLab), part of the NGO Atlantic Council, there was a 2.541 per cent increase in the number of TikTok followers, as well as a substantial increase in the number of likes, comments, and shares. In total, they estimate that he had a total of 1.4 billion views on TikTok globally.⁷⁴ Telegram was used to coordinate the campaign.

⁷¹ Munich Security Conference, 2024

⁷² The Constitutional Court of Romania, 2024

⁷³ Reuters, 2024

⁷⁴ Olari, 2024

To promote the candidate, the actor exploited a loophole in TikTok's rules against political advertising in that influencers were paid to share content that helped increase Georgescu's visibility, even though they did not necessarily mention him by name.⁷⁵ These influencers did not disclose their ties to the candidate. In addition to TikTok, shortcomings have also been identified in Meta's moderation of political advertising in connection with the Romanian elections.⁷⁶

Romanian authorities asked TikTok to take down Georgescu-related content four days before the first round of the election, as the content was not in line with campaign finance transparency legislation. TikTok claimed they had blocked Romanian users from these records. However, the documentation shows that Romanian users continued to have access, even on election day, which is a violation of the Election Act. This differential treatment increased Georgescu's exposure at the expense of other candidates.

In the aftermath of the election, the EU opened a case against TikTok based on the events of the Romanian election.⁷⁷

In addition to the use of social media, Romanian election IT systems were subjected to powerful attacks. Their intelligence services identified 85,000 cyberattacks against the Romanian IT system for the election. The aim was probably to gain access to data, change content and subjugate the system. The attacks continued for several days, including election day and the following day. The attacks came from 33 different countries, and it is difficult to attribute the attempts at influence to one specific actor.

Login credentials to Romanian election websites were posted on an illegal Russian cyber platform, as well as on a private Telegram channel known for spreading stolen data from state actors.

The Expert Group would like to emphasise that investigations into what happened in connection with the Romanian election are still ongoing and that new information may have emerged since the report was written. Although it is unclear to what extent AI was part of the picture in Romania, the events are illustrative of how influencing choices can take place, for example, by using algorithm-driven social media.

⁷⁵ Tray, 2024

⁷⁶ CheckFirst, 2024

⁷⁷ Blenkinsop, 2024

4.2 Finland

Finland held presidential elections on 28 January (first round) and 11 February (second round). As a Nordic country, Finland shares many similarities with Norway, including an extensive welfare state, a relatively high level of trust and a pluralistic media landscape with strong editorial control. At the same time, Finland has a geopolitical situation that differs from that of Norway. Finland shares a long border with Russia and did not join NATO until 2023.

The Expert Group visited Finland in the autumn of 2024 and met with various actors to gain an impression of the election. The clear impression is that (generative) AI did not play a major role in the presidential election.

4.2.1 Pre-election preparations in Finland

The Expert Group does not have the impression that AI in itself was a major part of the Finnish authorities' pre-election preparations, but that it was part of the overall efforts to secure elections. In this work, cooperation between various actors was particularly highlighted, and a cross-sectoral working group has been established to work on security in elections.

The election authorities emphasised that their role is not to classify real or fake news, but to ensure the provision of clear and correct information about how the election is conducted, and to be available to answer questions about this. In the event that the public technical solution reporting election results to the press and public should collapse as a result of attacks or technical problems, there is a backup solution located in another environment. One important aspect of the Finnish preparations was that this fallback solution should have a similar design to the original in order to avoid speculation or mistrust, as was noted in Sweden during their elections in 2018. At that time, the Swedish Election Authority's website was subjected to a data overload attack that led to allegations of electoral fraud as there were clear differences in the number of votes of certain parties when the site was back up compared to before it was taken down.⁷⁸

4.2.2 Events and lessons learnt from the election in Finland

Finnish voters can request a recount of their votes. There has been an increase in the number of people wishing to do this, but it is not possible to determine whether this increase is due to less confidence or other factors. The fact that all voting is done on

⁷⁸ Swedish Election Authority, n.d.; Vallgård, 2019

paper was emphasised as a strength in this respect, because it ensures that counting can take place in a transparent and generally unambiguous manner.

Although Finland has strong media that reaches a wide audience, social media has also become more important in the election campaign and as an arena for political discussion. In the Expert Group's meetings with Finnish actors, it was emphasised that far-right parties were particularly active on social media. They focus on targeting younger voter groups who are less likely to follow the news through editor-controlled media. A study conducted in connection with the Finnish election took a closer look at YouTube's recommendation algorithms and found an over-representation of right-wing recommendations. These recommendations appeared to favour videos related to the Finns Party and their candidates in particular, which the researchers believe indicates a bias in the algorithm.⁷⁹

Events in Finland in connection with the European Parliament elections are discussed in section 4.3.2.

4.3 Elections to the European Parliament

Elections to the European Parliament were held during 6–9 June 2024 in all 27 EU Member States. In practice, the elections to the European Parliament are not one single election, as the elections are conducted in each individual country based on election acts of each respective country. The EU has only laid down a few general guidelines for how representatives should be selected.⁸⁰

4.3.1 Preparations for the European Parliament elections

In the run-up to the election, there was concern about the role AI could play, particularly with respect to misinformation and disinformation. The EU has made wide-ranging efforts to prepare itself and the individual member states, which extend beyond the elections alone. The European Parliament has identified four pillars for these efforts:⁸¹

- Develop policies to strengthen democracy, make it more difficult for threat actors to misuse digital platforms and protect journalists and media pluralism.
- Spread awareness of disinformation and the EU's preparedness and response.

⁷⁹ Knuutila, Kuster and Lesplingart, 2024

⁸⁰ European Parliament, 2024a

⁸¹ European Parliament, 2024b

- Develop societal resilience to disinformation through critical media literacy and fact-checking.
- Cooperation with other institutions, national authorities or third parties.

In addition to measures implemented in connection with the election, there are also relevant regulations adopted by the EU through, among other things, the Digital Services Act (DSA) and the AI Act, which help ensure that the major technology companies, including platform providers and search engines, are subject to active content moderation and similar requirements, as discussed in Chapter 2.

Examples of actions taken by the EU include information on how to ensure free and secret elections on the European Parliament's election website, videos in different languages on the techniques used by threat actors to spread disinformation, and a toolkit for teachers on how to detect and counter disinformation. The European External Action Service (EEAS) has also established its own service that continuously monitors and exposes disinformation campaigns, called EUvsDisinfo.eu. This website, which is not limited to the European Parliament elections, publishes uncovered influence campaigns on an ongoing basis.

Prior to the election, all party groups in the European Parliament signed an agreement (Code of Conduct) in which they agreed to help ensure the ethical and transparent use of campaign tools and technology, including AI. Furthermore, the parties signed an agreement to refrain from using misleading content, regardless of whether it is AI-generated, to falsify candidates or other actors during an election. This agreement also stipulated that the use of AI-generated content should only be used if it is clearly labelled.⁸² The agreement was voluntary and non-binding, but parties and politicians were expected to comply with it out of loyalty. The agreement only covered political parties at European level and the national parties that actively signed it.

The Expert Group does not have a comprehensive overview of measures implemented by the individual member states, but is aware that both France⁸³ and Latvia⁸⁴ have introduced laws regulating the use of deepfakes, including in connection with elections. However, the Expert Group is not aware of what experience has been gained through

⁸² International IDEA, 2024

⁸³ Hogan Lovells, 2024

⁸⁴ LSM, 2024

the application of such laws, or whether any cases have been brought on the basis of these laws.

4.3.2 Events and experiences from the European Parliament elections

Based on the Expert Group's information about the European Parliament elections, there is no basis for concluding that AI had as great an impact on the election as many had feared. A report from the European Board for Digital Services concludes that measures to ensure preparedness and coordination were successful, and that no major or systematic cases of disinformation disrupting the election were uncovered.⁸⁵ The European Commission's preliminary review of known influence operations reported that AI had only been used to a minor extent in disinformation campaigns. In the weeks leading up to the election, it was found that approximately four per cent of all investigated and fact-checked disinformation was AI-generated. Political parties have used AI to a limited extent. Yet the experiences gained from the election demonstrates both the breadth of applications for this technology and its potential for manipulation.⁸⁶

The Alan Turing Institute conducted a survey of incidents where disinformation or deepfakes based on AI had gone viral in connection with both the European Parliament elections and the French parliamentary elections. Altogether, in these two elections only 11 such cases were uncovered, far less than many had feared in advance.⁸⁷ As these involved "viral" events, this refers to cases that have spread and received significant attention.

The Expert Group is not aware of election authorities, either at EU level or in individual countries, who have utilised AI in their own work in connection with election processes.

Misinformation from chatbots

In connection with the election, Democracy Reporting International conducted a survey on how four popular chatbots answered questions about the European elections. They conclude that none of these appear to be biased towards any of the parties or political sides. However, none of them were able to provide accurate information about the election process itself, i.e. about when the elections were held or how to vote.⁸⁸ A test

⁸⁵ European Board of Digital Services, 2024

⁸⁶ European Commission, 2024

⁸⁷ Stockwell, 2024

⁸⁸ Meyer-Resende, Davis, Denkovski and Allen, 2024

conducted by fact-checkers at Correctiv also found that chatbots provided erroneous information about candidates, as well as fabricated sources.⁸⁹

Amplification of negative stories on social media

In connection with the European Parliament elections, researchers from **Finland** conducted a study of how TikTok presented political information during the pre-election period.⁹⁰ Among users seeking information, search results contained offensive language about women and minorities. These were also biased by highlighting almost exclusively negative content about certain politicians. The researchers believe that TikTok's search results may have contributed to shaping what those searching for information on this platform see, and to maintaining prejudices. Another finding by the same study is that content from candidates dealing with controversial issues in domestic politics was more likely to be promoted in recommendations, while content on security and nature conservation was less likely to be promoted. The labelling of election-related content was also inconsistent.

AI-generated content by the far right

In the examples of the use of AI-generated content in the election campaign prior to the European Parliament elections, far-right parties in particular stand out as having created or contributed to the dissemination of fake content.

In **France**, the *Rassemblement National* (National Rally) party shared several AI-generated images. Through a campaign they called *L'Europe Sans Eux* [A Europe without them], AI-generated images were distributed and used to illustrate issues such as halting immigration and hijab use.⁹¹ Several far-right parties used AI-generated images as part of their campaign strategy.⁹²

The French website of the European party Identity and Democracy, one of the parties that had signed the agreement on the use of AI, also published AI-generated images of migrants, which were then shared on the party's social media channels. The party also posted several sponsored posts (advertisements) that consisted of videos with AI-generated content. One of these claimed that Europe is facing an "alarming migration

⁸⁹ Marinov, 2024

⁹⁰ Knuutila and Havula, 2024

⁹¹ Châtelet, 2024a

⁹² Schueler et al, 2024

crisis” and featured nine generated images depicting migrants, the EU flag and EU institutions, protests and explosions. According to Meta Ad Library, cited by DFRLab, the video had a reach of 29,406 users on Facebook and Instagram.⁹³

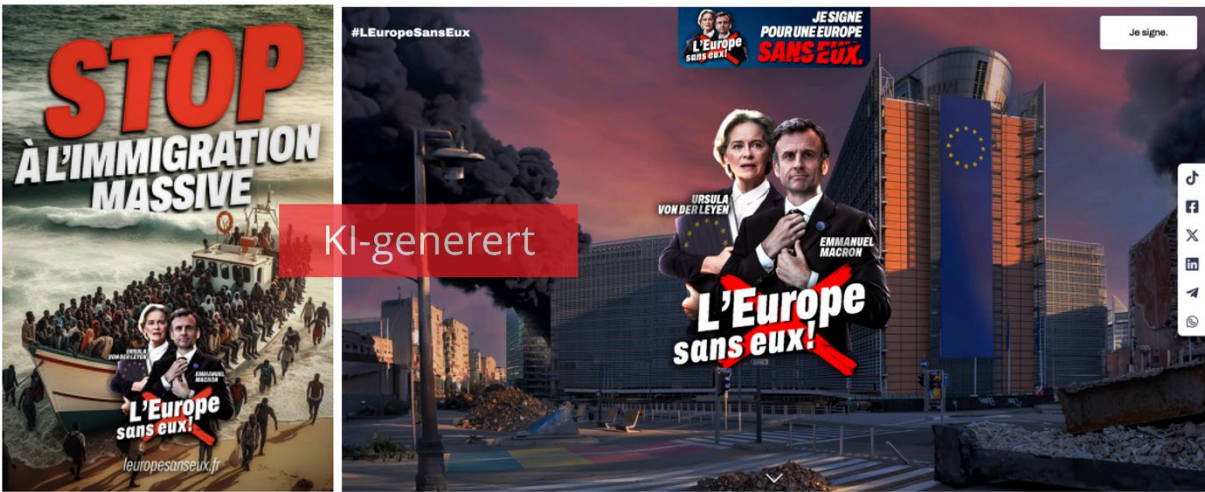


Figure 4.1 Examples of AI-generated content from the *L'Europe sans eux!* campaign. The Expert Group's labelling.

Source: Schueler et al. 2024

In **Italy**, Matteo Salvini, a member of the European Parliament and leader of the Lega party, utilised generative AI during this year's European Parliament elections. Salvini is known for his opposition to EU integration. The images were not labelled as AI-generated and were thus in violation of the European Parliament's agreement on AI use. One of the AI-generated images showed a pregnant person with a beard and the text "less Europe", and on the opposite side a seemingly heteronormative family with two children and the text "more Italy". Among other things, the image was used in a Facebook advertisement, which is believed to have cost of EUR 4,500–5,000 with a reach of three million users. Salvini also published several similar images, including one depicting French President Emmanuel Macron in a military uniform with an EU flag on his shoulder.⁹⁴

⁹³ Châtelet, 2024a

⁹⁴ Ibid.



Figure 4.2 Example of AI-generated content published on Matteo Salvini’s Instagram profile. The Expert Group’s labelling.

Source: Screenshot from Instagram, @matteosalviniofficial 23 May 2024

Although Salvini and his Lega party were not bound by the agreement signed between the parties of the European Parliament, there have been reactions to his use of AI-generated images. The criticism primarily focuses on the use of AI in political communication, their election campaign strategies and the use of AI-generated content without sufficient labelling or transparency. Some X users have pointed out that such strategies could undermine trust in political messages and reinforce divisions in society.

In **Germany**, the Alternative for Germany (AfD) party ran ad campaigns on Facebook and Instagram. At least three of these are said to have been manipulated using

generative AI. One of the images shows a white woman with visible bodily injuries and the text: “the connection between migration and crime has been denied for years”.⁹⁵

Fake websites

Activity in the pro-Russian Doppelganger operation (see discussion in Box 3.1) increased during the period leading up to the European elections. This included content about the election itself. In the run-up to the election, fake versions of well-known news media such as *Die Welt*, *Le Parisien*, *Polskie Radio* and several others were identified.⁹⁶ OpenAI revealed that people associated with the Doppelganger operation used their tools to generate comments in different languages for social media, to translate and edit articles posted on websites, to generate headlines and to turn stories into Facebook posts.⁹⁷

4.4 The United Kingdom

The United Kingdom held a general election on 4 July 2024. The use of generative AI during the election was limited and relatively few examples were registered.

Despite an increase in digital campaigning since the last election, the impression is that political parties in the United Kingdom mainly focused on traditional campaigning methods. Editor-controlled media remains strong, but trust in the media is declining. It is clear that younger generations are drawn to social media for their news consumption.

4.4.1 Preparations prior to the election

As part of the pre-election risk assessment, the UK Electoral Commission (UKEC) invited Microsoft, OpenAI and social media actors, among others, to participate in a dialogue, where the purpose was to learn how they would organise their work prior to the election. However, this dialogue was not formalised. In practice, this means that the platforms are largely free to decide whether they wish to accept input. They also have the power to define what should be considered disinformation within an electoral context.

The National Cyber Security Centre (NCSC) began its preparations a year before the election was held. Preparations included scenario planning, risk analyses, social media data scraping, identifying gaps in data systems, and providing guidance and support to

⁹⁵ Elliott, 2024a

⁹⁶ EUvsDisinfo, 2024

⁹⁷ OpenAI, 2024

political candidates. A set of voter profiles was also identified, which could provide the direction for discussions, as well as an indication of how different people respond differently to digital content. In addition, NCSC prepared how to deal with hack and leak operations, which targeted email systems and user accounts.

One of the specific focus areas was to strengthen preparedness against targeted campaigns aimed at population groups that could effectively share misinformation about the election, as well as campaigns that could intentionally reinforce divisions in society.

The actors the Expert Group met with in the United Kingdom also mentioned the ongoing efforts to strengthen the population's critical understanding of the media, political expertise and knowledge about election processes. Such expertise was cited as particularly important for ensuring that AI-generated content does not spread or lead voters to be deceived by fake content or false claims.

4.4.2 Events and lessons learnt from the UK election

The Alan Turing Institute found 16 confirmed and viral cases of AI-generated disinformation or deepfakes during the UK general election. Among the specific threats highlighted by AI are smear campaigns, misleading political advertising, voter targeting, parodic and satirical content, AI-generated information sources and misattributions of AI.⁹⁸

During the UK election, there were several instances of parodic deepfakes that could be perceived as genuine. There were also examples of content in the grey area between satire and disinformation, such as an AI-generated falsified audio clip of Labour's prime minister candidate Keir Starmer allegedly berating staff. This fake audio clip was quickly uncovered before it had spread far and therefore received little attention.

There were also instances of harassment and smear campaigns targeting politicians. Certain female politicians were subjected to smear campaigns in which AI tools were used to create pornographic images.⁹⁹ Deepfakes can have significance even if they have been discredited. This also applies to fake audio clips. The Mayor of London, Sadiq

⁹⁸ Stockwell, Hughes, Swatton and Bishop, 2024

⁹⁹ Newman, 2024

Khan, stated that an AI-generated falsified audio clip had been a significant burden for him.¹⁰⁰

Far-right activist Tommy Robinson shared an image on X to discredit Keir Starmer and Labour, using a generated image to illustrate that the party was no longer on the side of the workers.¹⁰¹



Figure 4.3 AI-generated image shared by far-right activist Tommy Robinson on X. The Expert Group’s labelling.

Source: Screenshot of AI-generated image posted on X by @TRobinsonNewEra on 10 June 2024

During the Expert Group’s meetings in the United Kingdom, it was noted that chatbots had given incorrect answers to questions about the election, for example about ID

¹⁰⁰ Spring, 2023

¹⁰¹ Williams, 2024

requirements for voting. The fact that chatbots did not always give correct answers about the election is also confirmed by a survey from the Reuters Institute, which shows that a significant proportion of chatbot answers were either entirely or partially incorrect.¹⁰² Several actors also referred to the development of copyright labelling of content as an important measure to strengthen the credibility of true information.

One example of the use of AI by candidates was the stunt by candidate Steve Endacott, who introduced himself using an AI avatar called “AI Steve”. People could “chat” with the candidate through this avatar about issues that were important to them. On the other end, the candidate could use this tool to determine his positions on issues if elected.¹⁰³

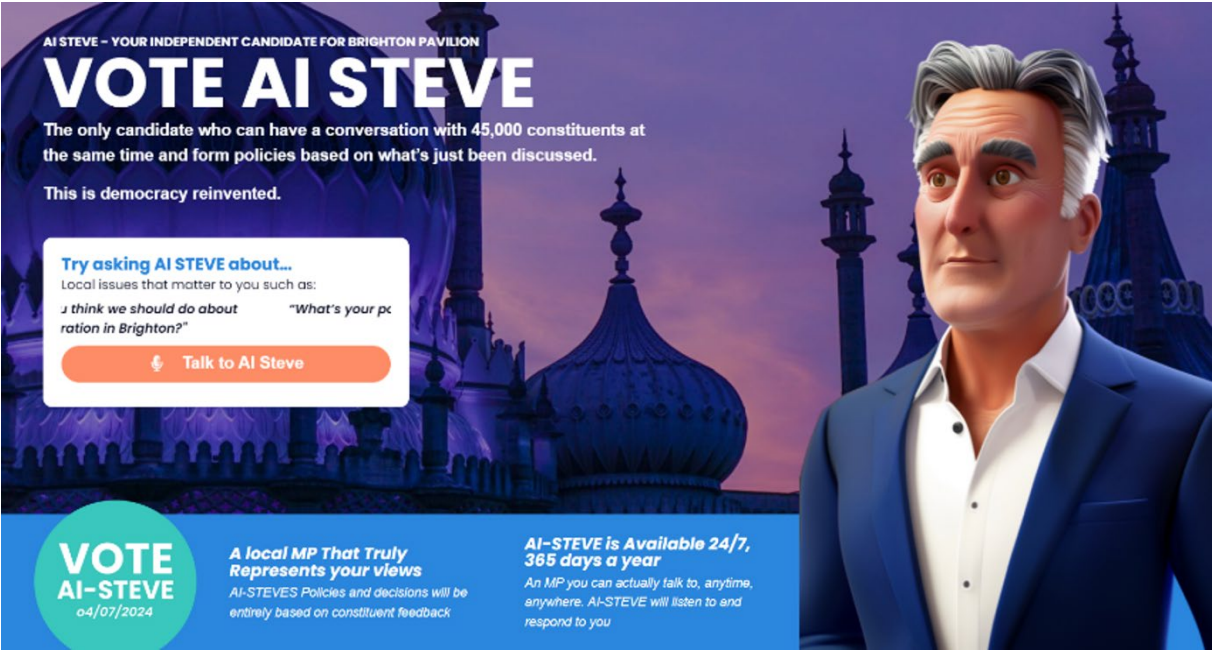


Figure 4.4 Screenshot from the “AI Steve” website.

Source: www.ai-steve.co.uk

The United Kingdom has sanctioned Russia-linked networks that are part of the Doppelganger operation (described in Box 3.1). The Social Design Agency (SDA), one of the sanctioned actors, is behind the production of at least 120 fake websites that mimic genuine news sources and government websites, with the aim of misleading users, promoting Russian narratives and influencing election processes.¹⁰⁴

¹⁰² Simon, Fletcher and Nielsen, 2024

¹⁰³ Elliott, 2024b

¹⁰⁴ GOV.uk, 2024

A new challenge highlighted during the Expert Group's meetings in the United Kingdom was the emergence of ad hoc organisations set up to run short-term campaigns. While the party organisations themselves are likely to have a high threshold for using AI in unethical ways, it is feared that such loosely associated organisations may have a lower threshold for AI use.

4.5 The United States

The United States held both presidential and congressional elections on 5 November 2024. At the same time, many elections were held at the state level and for various offices at lower levels. Occurrences in the United States show that generative AI had an impact on the information landscape and made its way into the political agenda. Lessons learnt from the United States also emphasise the importance of ensuring that election authorities have the sufficient resources and expertise to deal with the challenges associated with AI – and to take advantage of the opportunities it brings.

Elections in the United States are highly decentralised, with each state having its own rules on how elections are conducted. There are major differences with respect to voter registration, voting procedures and the resources and expertise of local election authorities. At the federal level, the Help America Vote Act (HAVA) set only a few minimum standards that states must follow.¹⁰⁵

4.5.1 Preparations prior to the elections

There are many actors involved in the organisation of US elections and it has not been possible to get an overall picture of all preparations made in every state. The Expert Group has therefore primarily focused on what has been done at the federal level, as well as on some much-discussed measures at the state level.

The United States Election Assistance Commission (EAC) provides guidance on the requirements of the Help America Vote Act. Ahead of this year's election, the EAC prepared information about AI for the electoral authorities as a contribution to expertise and awareness at the various levels. As part of their work, they also created an AI toolkit for election officials that focused on the importance of AI for communication. It contained examples and templates for materials that authorities at different levels could use and showed where voters could get quality-assured information about the

¹⁰⁵ United States Election Assistance Commission, 2023

election.¹⁰⁶ Other actors also produced materials for election authorities on AI and security.¹⁰⁷

Security authorities such as the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of the Director of National Intelligence (ODNI) are responsible for election security, including foreign influence. In addition to work done at the intelligence level, which is often classified, security authorities also carried out extensive activities aimed at key actors in elections at the state level and below to assist them in their security efforts leading up to the election.¹⁰⁸

The Expert Group is also aware that exercises were conducted in several states prior to the election, where AI was included in some of the training scenarios, both with assistance from CISA and from other actors. For example, the non-profit organisation Bipartisan Policy Center conducted exercises that brought together personnel from state and local election authorities and key actors from other sectors and institutions to discuss how election authorities could respond to hypothetical scenarios involving AI and elections.¹⁰⁹ In Arizona, exercises were carried out with local election workers based on scenarios with fake calls where deepfake technology was used to clone voices directing polling stations to close early or to deliver ballots to the wrong place.¹¹⁰

In several states, including California, bills were introduced to ban or regulate the use of deepfakes in connection with elections. However, it proved challenging to get such laws passed, partly due to strict freedom of speech laws.¹¹¹

4.5.2 Events and lessons learnt from the US election

The United States has a highly polarised information and media landscape along political dividing lines and few or no common arenas for the public exchange of information and opinions. This means that different sides in politics receive news and information about political issues from different sources, and they rarely listen to or

¹⁰⁶ United States Election Assistance Commission, 2024

¹⁰⁷ See e.g. Gorman and Levine, 2024

¹⁰⁸ Cybersecurity and Infrastructure Security Agency, 2024

¹⁰⁹ See e.g. Jackson, Weil and Adler, 2024

¹¹⁰ DGA Group, 2024

¹¹¹ Katzenberger, 2024

trust sources perceived to be from the political opposition. One striking development that was also observed during the 2024 election was that the candidates rarely appeared in editorial media and instead prioritised other platforms, such as social media, YouTube channels and podcasts led by well-known profiles.¹¹²

Several threat actors attempted to influence the US election, including Russia, China, and Iran. Although the extent to which such actors have used AI remains unknown, several of the actors the Expert Group met with in the United States stated that the more traditional methods of influence are still being used and can work well, and rather than representing something groundbreaking, AI tends to reinforce existing challenges. At the same time, it was emphasised that we are still in the early stages of AI development, and that we therefore cannot write it off as a potential major threat in the future.

Examples of incidents

There were many events in the run-up to the election where AI was utilised. Some of the content was particularly characterised by satire or entertainment. However, there were also examples of content that indicated a more strategic use of AI tools. In an analysis of 582 cases of fake content in the presidential election campaign, cited by the Washington Post, researchers at Purdue University found that 33 per cent were about Trump, 16 per cent about Harris and 16 per cent about Biden. This included content of both a positive and negative nature.¹¹³

In the wake of Hurricane Helene, which hit the southeastern coast of the United States just weeks before the election, images were shared showing Donald Trump present in the affected areas. These images were widely circulated, despite being quickly revealed that the images were fake.¹¹⁴ This content helped reinforce emotions and impressions, and supported subjective views of reality as one might *feel or perceive* it to be. This indicates that AI can reinforce perceptions even if the recipient understands that the content is fake.

¹¹² Stocking, et al, 2024

¹¹³ Verma, Oremus and Zakrzewski, 2024

¹¹⁴ Hudnall, 2024



Figure 4.5 AI-generated image of Donald Trump that circulated in connection with Hurricane Helene. The Expert Group's labelling.

Source: Screenshot of AI-generated image posted on Facebook by Steve Youell on 30 September 2024

AI-generated content was also used to smear candidates. For instance, there were several images portraying Kamala Harris as a communist. Kamala Harris's voice was also falsified, and in July Elon Musk shared a fake audio clip of her celebrating Biden's resignation and referring to herself as a "diversity hire". This audio clip was viewed more than 100 million times.¹¹⁵

¹¹⁵ Verma, Oremus and Zakrzewski, 2024



Figure 4.6 AI-generated image portraying Kamala Harris as a communist. The Expert Group's labelling.

Source: Screenshot of AI-generated image posted on X by @realDonaldTrump on 18 August 2024

During the election campaign, Trump himself also shared fake images that allegedly showed that Taylor Swift was supporting him. Among the images shared was one depicting Swift as Uncle Sam (a well-known American symbol personifying the United States and the US Government), with the caption "Taylor Wants You to Vote for Donald Trump". Other AI-generated images depicted Swift fans wearing t-shirts that read "Swifties for Trump."¹¹⁶ Swift subsequently publicised her support for Kamala Harris, pointing out that the high-profile fake photos made it all the more important for her to clarify her actual position.¹¹⁷

¹¹⁶ Vigdor, 2024

¹¹⁷ Nehamas, Schleifer and Corasaniti, 2024

During the Democratic primary, voters in New Hampshire received automated calls with a voice clone of President Joe Biden. In these calls, Biden reportedly asked voters not to vote in the primary election in order to save their votes for November.¹¹⁸ These calls were quickly revealed as fake, but this AI voice cloning is one example of how AI can be used to influence voters. Both the company that offered the platform used for the fraudulent calls and one individual have been fined for the incidents.¹¹⁹

Several fake news websites promoting Russian narratives in the United States have been revealed, including one called “D.C. Weekly”. On the surface, the site might appear to be an ordinary news website, but in reality, it has been used to promote Russian narratives, partly by spreading false claims about the Ukrainian president’s spending. Researchers investigating the site found that language models were being used to paraphrase articles from other news sites.¹²⁰ Even if the stories on such pages do not necessarily reach a large audience, they can be picked up and spread further, primarily through social media. See Box 3.1 for information about the Doppelganger operation.

In 2024, it became known that the media company Tenet Media received funding from, and was basically controlled by the Russian state-controlled news network RT. Tenet Media used influencers who created content for the platform, although the influencers themselves were unaware of its Russian connections. Tenet Media produced over two thousand videos with more than 16 million views on YouTube. Most of the videos supported Russian interests and focused on divisive issues, partly to weaken American support for Ukraine. This example shows how state threat actors can pay influencers to present a message on their behalf.¹²¹

Another way in which AI played a role in the US election was by using what is known as the “liar’s dividend”. This concept describes a situation where someone claims that genuine content is AI-generated, often in order to discredit or disclaim responsibility for

¹¹⁸ Matza, 2024

¹¹⁹ Associated Press, 2024

¹²⁰ Linvill and Warren, 2023

¹²¹ Gotfredsen, 2024

the content.¹²² One example was when Trump falsely claimed that photos from Harris's rallies were manipulated to give the impression of a larger audience.¹²³

4.6 Individual events from other elections

In addition to the elections referred to above, the Expert Group will in the following highlight individual events from other elections that illustrate how AI contributed to characterising elections in 2024.

Parliamentary elections in Croatia

Croatia held parliamentary elections on 17 April. The election was characterised by several instances of AI-generated disinformation, particularly on social media such as TikTok and X, where the information was targeted at political actors.

Generative AI was used during and after the Croatian parliamentary elections in 2024. A total of 19 cases of disinformation were identified in a survey conducted by the Adria Digital Media Observatory (ADMO).¹²⁴ In May 2024, 18 of the 19 uncovered cases were still accessible and none of them were labelled. These cases were spread via TikTok and X, and they could be traced back to private profiles. The disinformation often involved a combination of generative AI and 'cheapfake' technology. The most frequent form of disinformation was manipulated audio tracks in videos (16 cases), followed by manipulated videos (2 cases), while only one AI-generated image was found.

The disinformation that was spread primarily concerned the political elite and was, in many cases, satirical in nature. ADMO highlights three incidents:

- A video on Instagram Reels where Prime Minister Andrej Plenković appears to be encouraging citizens to buy shares in an oil company co-owned by the Croatian government. The video was taken from a genuine press conference, but the soundtrack is falsified.
- Plenković and the Croatian Democratic Union (HDZ) party were parodied in a video published by a satirical show presented on X. Through a deepfake video using an official HDZ advert with manipulated sound and subtitles, Plenković makes statements about HDZ's dishonesty and corruption and encourages voters to smile and vote for them.

¹²² Chesney and Citron, 2019

¹²³ Goldmacher, 2024

¹²⁴ Brautović and Roško, 2024

- In a TikTok video, President Zoran Milanović was portrayed making a fake statement about his alleged love of gambling and slot machines. This example also utilises a combination of genuine footage from a press conference together with fake audio.

Parliamentary elections in France

French voters went to the polls in 2024 in two elections: the European Parliament elections in June and new elections to the National Assembly with two rounds of voting in June and July, respectively. Since the elections were held at more or less the same time, it is not necessarily easy to distinguish which election was concerned with which issue. Events directly related to the European Parliament elections are discussed in section 4.3.2.

In connection with the election to the National Assembly, fake websites were uncovered that most likely originated from Russian influence networks. In June, a website posing as the website of President Macron's party, Renaissance, was uncovered. This fake website made false claims that people who voted for the party would receive a reward in the amount of EUR 100. The website was promoted through a fake news website using AI-based language models to create content. In several articles, the prompt (the instruction given to the AI tool) that was used was openly available online, which indicated that the language model was to rewrite authentic news stories to take a conservative stance against Macron's government. According to DFRLab, the campaign was likely linked to the Russian CopyCop operation.¹²⁵

State elections in Germany

In 2024, state elections were held in three German states in September. Several German political parties have utilised AI in their communications. In connection with campaigns in the states of Saxony and Thuringia in September 2024, the German TV channel ZDF conducted a survey on the use of AI in election campaigns.

The survey showed that nearly all political parties used generative AI, but that there was no clear evidence of the systematic use of AI in election campaigns. They found that the parties used AI in a number of ways, such as for texts, image editing, analyses and generating music for election campaign videos. They also found that the Alternative for

¹²⁵ Châtelet, 2024b

Germany (AfD) and Free Democratic Party (FDP) parties have used their own AI-powered chatbots on their websites to answer questions about their election manifestos.¹²⁶

Presidential election in Moldova

Moldova held a presidential election in October and at the same time held a referendum on the EU. Moldova was subjected to attempts at influence by Russia, which in addition to attempts at vote buying and other “traditional” methods, also involved the use of AI. Among other things, an extensive use of AI-based bots that posted comments on Facebook was uncovered. Deepfakes were also shared by President Maia Sandu, including a call to vote for a pro-Russian candidate. Despite a major campaign to influence the election, the attempt was considered a failure.¹²⁷

Parliamentary elections in Georgia

Like Moldova, the Georgian parliamentary elections in October were also subject to extensive attempts at influence. A report from the NGO International Society for Fair Elections and Democracy (ISFED) found that anonymous actors used AI to create deepfakes of politicians. TikTok in particular was used to distribute these, which included falsified voices of President Salomé Zourabichvili and former Prime Minister Giorgi Gakharia, as well as AI-generated images to illustrate what the state of the country would be should the former government return after the election.¹²⁸

General election in South Korea

The South Korean general election was held on 10 April 2024. In the run-up to the general election, South Korea implemented a number of measures to regulate the use of AI and counteract the spread of disinformation. In January 2024, its National Assembly passed a ban on AI-generated deepfakes in political campaigns 90 days before elections. The National Electoral Commission (NEC) has established guidelines for clear labelling, also outside this 90-day framework. The NEC has also set up an AI expert group, whose main task is to monitor and manage the misuse of AI during election processes.

AI-manipulated content and fake news is a widespread problem in South Korea with social media being a major source of the spreading. In March 2024, a deepfake of

¹²⁶ Scholl, 2024

¹²⁷ Scott, 2024

¹²⁸ International Society for Fair Elections and Democracy, 2024

President Yoon appeared, in which leaders of his party were apparently criticising the opposition party. Despite the new restrictions on the use of AI in election campaigns, more than 380 offences related to deepfakes were uncovered between January and April. Of these, 181 cases were only reported during the last 15 days before the parliamentary elections.

South Korea's leading search engine, Naver, has implemented stronger monitoring to counter new forms of misuse, including AI-generated comments and deepfakes. The platform has also introduced features that allow users to report election misinformation directly, with a dedicated reporting centre established to streamline communication with the NEC.

General elections in India

India conducted general elections in different phases from April to June 2024. The elections were largely peaceful but also characterised by a changing information landscape and the use of new technology.

Prime Minister Narendra Modi and his party utilised AI themselves in their communications. A deepfake of Modi targeting voters at an individual level was shared through the messaging service WhatsApp. This was tailored to each recipient with personalised messages and in the recipient's preferred language. Thereby, AI was used to personalise information in a new way to reach voter groups in their native language.¹²⁹

General elections in Pakistan

Pakistan held general elections in February. The main opposition party, PTI, used AI to mobilise voters, mainly to get party leader Imran Khan's message across. Khan has been imprisoned since August 2023, with limited access to journalists, media and the outside world. Therefore, the party used generative AI and deepfake technology both during and after the election campaign, with voice cloning and a generated video where Khan appeared to be speaking, although this was based on notes he was able to send from prison.¹³⁰

¹²⁹ Raj, 2024

¹³⁰ Zhuang, 2024

5 Changes in the challenges facing Norwegian elections

In this chapter, the Expert Group will assess the significance of AI in a Norwegian electoral context. This is done by first assessing which international events from 2024 may be relevant in a Norwegian context, and then extrapolating and highlighting the most significant challenges the Expert Group believes we should be aware of.

As shown in Chapter 4, there have been a number of incidents involving the use of AI in the 2024 election year, although it must be emphasised that generative AI did not become the dominant factor as feared at the start of the year. Nevertheless, it is clear, both from the meetings held by the Expert Group and from other sources, that we are still in an early phase of AI development. It will likely still be some time before the technology itself and the actors that use it are able to realise its full potential.

Box 5.1 Technological developments leading up to the 2025 election

AI technology is changing rapidly, and so, it appears, is its use. However, we are not yet aware of its full potential. In the run-up to the parliamentary election in 2025, the possibilities and availability of the technology may increase.

AI tools will increasingly become part of smartphones' operating systems. This allows for greater use by the general public for both editing and generating text, images, audio, and video.

AI agents, i.e. programmes based on language models that can perform various tasks, could become more widespread and help improve the productivity of a number of actors, including threat actors. The use of chatbots as information sources may also increase. Search engines and social media are expected to become progressively AI-driven and more of the information landscape will be filtered through AI systems.

Such changes could increase the impact of AI on elections, increase the prevalence of misinformation and disinformation, and enhance the efficiency of influence operations. It is natural to expect that actors, both threat actors, as well as parties, authorities and individuals, will over time learn to make far more use of the technology's possibilities.

5.1 The information and media landscape

AI-generated content was not as widespread and significant for the 2024 elections as many had feared, but documentation shows that AI has a clear impact on the

information and media landscape around elections. It is within this main area that the Expert Group believes it will find the most distinct changes in the situation.

Overall, many of the observed examples of AI-generated content from the last election year are of a humorous nature or blatantly false, and clearly within the bounds of freedom of expression. Much of the content is not necessarily designed to be persuasive. Several examples, such as the fake photos of Trump in connection with Hurricane Helene and the fake videos from the Croatian elections, show that the primary function of such content is to create impressions and spur emotions in the viewer. Thereby, it can help paint a positive or negative picture of a candidate or issue. This content has been spread on social media platforms.

In terms of the wider media landscape, there are different factors pulling in different directions. The US incidents in particular are closely linked to the fact that, over time, American media have had an increasingly weak position and become far more polarised along political lines. Algorithm-driven and engagement-driven social media have become increasingly important. These play an increasingly important role in voters' access to information, rendering them more vulnerable to misinformation, disinformation, and covert influence campaigns. The example from Romania also shows how social media algorithms can be exploited.

The Norwegian media system, with its independent, editor-controlled and diverse media frequently being used by the population, is a good starting point for resilience against both the increasing polarisation and fragmentation of society, and against unwanted influence by AI-generated content and AI-controlled operations in connection with elections.

In Norway, we have a strong national media system with a high level of trust and, not least, with a high coverage of local media. Nevertheless, both in Norway and Europe in general, there are clear signs that the role of editorial media is under pressure from social media and is changing media habits. This is especially true among young people, who are more likely to use social media and AI services, and less likely to use editorial media.¹³¹ In the face of the challenges posed by AI, it will therefore be crucial to maintain the societal role of editor-controlled media and access to quality-assured information, especially for new generations.

Editor-controlled media have become increasingly dependent on social media and AI-driven algorithms in order to reach young users. They are also gradually being replaced

¹³¹ See e.g. Lüders and Sundet, 2022

by chatbots and AI searches that are often trained and based on information produced by editor-controlled media. If users move from the editor-controlled information sphere to AI and algorithm-controlled platforms, the power of the Norwegian media model, and people's use of the media, community arenas and public debate will all be reduced.

The growing prevalence of AI-generated content will lead to a greater need for strengthening critical media literacy and source awareness in the population. There are several actors working on fact-checking and developing an awareness and understanding of critical media, technology, and AI. In Norway, we have the Norwegian Media Authority, Faktisk.no and its education department – Tenk, as well as an initiative for a centre for source awareness. One challenge is to ensure that critical media literacy programmes reach those who actually have the greatest need and who are most exposed to misinformation and disinformation.

In the following, the Expert Group will highlight specific changes in the challenges facing the information and media landscape:

5.1.1 Increased levels of misinformation and disinformation and reduced trust in information

AI technology is reviving the significance of social media for the information landscape in democracies and challenging them in three specific areas. Firstly, the content that users are exposed to is governed by algorithms and data on user interests, interactions and demographic data, and on what others in their social media network are sharing. This means that different users are presented with different content, even when using the same platform. Secondly, this way of prioritising content may contribute to an increase in the spread of misinformation and disinformation, as there is no quality control. Thirdly, generative AI tools provide more opportunities for content production, as well as faster distribution through social media.

Increased prevalence of generated content can make it more difficult to distinguish between what is true and false, and contribute to reducing overall trust in information. In connection with elections, where there is an enormous need for information about the election, issues, parties and candidates, such developments would pose a serious challenge.

Most AI-generated content that is created and distributed is not illegal. However, it can be undesirable, particularly if it serves to blur the distinction between truth and falsehood and create confusion. Therefore, it may be necessary to be prepared for how to accommodate this type of use of AI, without it doing so in a way that reduces freedom of expression or the actual opportunities to express oneself. One of the big questions that will determine the entire information landscape in the years to come, not only

limited to elections, is how to ensure the authenticity of content when we don't know for certain whether text, images, audio, or video are genuine in the first place.

One development that the Expert Group has noticed is that the attention AI has received through the *super election year* of 2024 may in itself have helped to challenge trust in the information landscape. This can happen when attention leads to excessive fear and suspicion, so that any and all information is considered uncertain.

As an extension of this, there were also examples in the US election campaign of claims that actual events were fabricated, such as when Donald Trump claimed that photos of the crowds at Kamala Harris's rallies were faked to appear larger than they actually were. Claiming that documentation of actual events is fabricated could allow someone to shy away from uncomfortable situations. Such examples of the liar's dividend can contribute to confusion and further blurring of the distinction between truth and falsehood, and can thus become a problem.

These trends can challenge democracies by creating a more cluttered information landscape, where personalised and rapidly generated content could influence public debate, weaken a shared understanding of reality and pave the way for manipulating public opinion.

5.1.2 Changes in sources of information used

In Norway, the position of editor-controlled media is still strong, but it is important to take the shift towards algorithm-driven social media and AI-based chatbots as sources of information seriously — also in Norway.

There are many examples from the 2024 elections that indicate the need for great caution when using chatbots as a source of information on election-related issues. Both the United Kingdom and European elections had documentation of chatbots providing incorrect or inaccurate information to questions about the elections. At the same time, chatbots are becoming increasingly widespread as a source of information, and some people, especially the younger demographic, are preferring to use chatbots or social media rather than traditional search engines.¹³²

¹³² Hofsrud, 2024

Når kan jeg stemme til stortingsvalget i Norge i 2025 (dato og klokkeslett)?



Stortingsvalget i Norge 2025 vil finne sted den **14. september 2025**. Stemmegivning kan normalt foregå fra klokken 09:00 om morgenen til 21:00 om kvelden på selve valgdagen.

I tillegg er det mulig å forhåndsstemme fra 10. august til 10. september 2025, avhengig av hvor du befinner deg. Dette kan gjøres på forhåndsstemmesedler i kommuner rundt om i landet.

Figure 5.1 Screenshot showing that ChatGPT gives incorrect answers to questions about the date of the 2025 election day. The correct date is 8 September.

Source: Screenshot from ChatGPT

MEG

Når kan jeg stemme til stortingsvalget i Norge i 2025 (dato og klokkeslett)?

MY AI

Du kan stemme til stortingsvalget i Norge den 13. september 2025. Valglokalene åpner vanligvis kl. 09:00 og stenger kl. 21:00. Husk å sjekke nærmere informasjon når datoen nærmer seg! 📦

Figure 5.2 Screenshot showing that Snapchat's MyAI gives incorrect answers to questions about the 2025 election day. The correct date is 8 September.

Source: Screenshot from Snapchat's MyAI

In a simple test conducted in connection with the Expert Group's work, ChatGPT stated that the 2025 parliamentary election in Norway will be held on 14 September, i.e., almost a week later than the actual election day, which is Monday, 8 September (see Figure 5.1). Similarly, Snapchat's MyAI answered that election day is 13 September, which is also incorrect (Figure 5.2). Such errors, if not corrected by other sources, could mean that some voters will not have the chance to vote. In several of the countries visited by the Expert Group, the role of electoral authorities as providers of accurate and verified information about the elections was emphasised. These examples highlight the necessity for election authorities to ensure that accurate information about the election reaches a wide audience.

In the future, several actors will likely also offer AI-driven searches, which could add filters between users and sources of the information, thereby making the source of the information less apparent.

The media offer voting advice applications during Norwegian elections, and these are actively used by many people when making decisions on what party to vote for. In fact, 50 per cent of voters under the age of 34 mention voting advice applications as an important source of information.¹³³ By 2024, the media will have tested different ways of using AI in election coverage, and the Expert Group expects to see the emergence of voting advice applications that rely on AI to a greater extent than before. The Expert Group also expects political parties to test different ways of using AI in their election campaigns, such as chatbots that can answer questions about a party's policies. As with any use of new technology in connection with elections, the Expert Group wishes to emphasise the importance of thorough testing to ensure that the developed tools function as intended.

5.1.3 Misrepresentation of people and events

In the public debate on AI and elections, deepfakes in particular have taken centre stage. False representations of people or events have also been possible in the past, but this is an area where AI has truly opened up opportunities for this to be done quickly and without any special expertise or sizeable resources.

The unethical use of AI for creating such false representations is something the Expert Group expects could also occur in Norway. It is not first and foremost the well-

¹³³ Kleven and Bergseteren, 2024

established parties we expect will use AI in this fashion. In doing so, they would run the risk of damage to their reputation and reduced confidence in the party's ability to campaign fairly. The parties in the Norwegian Parliament have already entered into a joint agreement where they pledge not to produce, use or disseminate deepfakes with fabricated messages from other parties, politicians or social actors.¹³⁴ The main risk of AI-generated content being used in unethical ways is therefore more likely to come from other actors who want to highlight a position or party, for example, as short-term campaigns from loosely associated or informal groups and organisations, or from parties or political networks on the political fringes.

Certain politicians may be particularly vulnerable to being misrepresented in deepfakes as we saw from the examples in the United Kingdom, where female politicians were subject to sexualised deepfakes. We do not have any information about similar situations in Norway, but surveys on hatred and slander directed at politicians show that some are more vulnerable than others.¹³⁵ In the Expert Group's opinion, there may be reason to be prepared for the eventuality that also these individuals could be exposed to smear campaigns made possible by deepfake technology. Others, such as public officials, celebrities, and journalists, may also be exposed to false representations that could lead to negative consequences.

In the United States, Taylor Swift's fabricated endorsement of Trump's candidacy is a good example of how celebrities can also be subject to false representations. In both the United States and Norway, there are many examples of celebrities participating in political parties' election campaigns. However, it becomes far more problematic if this apparent support is not authentic, as celebrities can be highly influential. Nevertheless, we do not consider this to be the primary risk, as the fake use of celebrities is likely to be swiftly uncovered. A greater risk is the falsifying of lesser-known individuals, who may still have significant influence or importance for the election, but may not be detected as easily or quickly.¹³⁶ One hypothetical example, presented during one of the Expert Group's meetings in the United States, was if the voice of a local election official was used in fake phone calls to polling stations, for example with messages to stop the voting process.

¹³⁴ IKT Norge, 2024

¹³⁵ See e.g. Brandtzæg et al., 2022 and Ipsos, 2023

¹³⁶ Coldewey, 2024

In several of the AI examples from 2024, it is clear to most people that the content is not real. For example, most people realised that Donald Trump could not have been present during the rescue work following Hurricane Helene. However, such obviously false images may also have an effect, which indicates that content does not have to be perfect or realistic. An effect can be achieved when the content is likely to create impressions and emotions in the viewer, or if the content illustrates something the recipients believe to be “true”, e.g. that Trump would do more than the Biden administration did to help victims, even if this is not really the case.

5.1.4 Greater dependence on powerful technology companies and platforms

The shift from editor-controlled media to social media and other technological platforms means that we as a society are becoming more dependent on technology companies to facilitate an infrastructure for information sharing in connection with elections. When platforms are important sources of information, this requires information that is important to communicate to be made available on said platforms. However, this has proven challenging in practice.

Technology companies have a substantial amount of power as they have large financial resources and direct access to users and user data, which means they can determine the conditions for the information environment in which we operate. While social media was initially seen as democratising and decentralising, the trend is now towards centralising power in the hands of a few major actors. This power can be illustrated by the fact that Google has conducted tests in several countries, including Denmark, where a sample of 1 per cent of the users were unable to get results from EU-based news sources.¹³⁷ As a small country, Norway has limited influence over how the platforms operate, and these have a minimal presence in the country. In regulating them, we therefore rely on the regulations established at the EU level, and that relevant legislation is swiftly incorporated into Norwegian legislation.

Based on The Industry Standard Against Disinformation, the platforms report on their efforts to prevent the spread of disinformation on their platforms. The Norwegian Media Authority's assessment from September 2024 particularly indicates Meta as a problematic platform, as that they do not report figures for Norway and the figures provided are approximate and not consistent according to the level to which they apply.¹³⁸

¹³⁷ Connal, 2024

¹³⁸ The Norwegian Media Authority, 2024c

In meetings with the Expert Group, several political parties mentioned that their communication with technology companies is challenging. There are several reasons for this, but they are particularly perceived as inaccessible and difficult to contact when necessary, e.g. when the parties profiles have (incorrectly) been taken down. Now that social media platforms have become important for political parties, it is problematic for them if they lose access to their own channels, especially during an election campaign. This would require swift action from the platforms, although based on past incidents, such cases are not sufficiently followed up. Several parties have described this issue to the Expert Group. Meta's handling of the removal of the Facebook page of the Norwegian Centre for Holocaust and Minority Studies is an illustrative example of how a page can be taken down without telling the owner why or getting in touch with the platform to discuss how it can be restored.¹³⁹

The Expert Group believes that the expanding power of technology companies is reducing national autonomy. They have become an increasingly important part of the infrastructure for public dialogue. Technology companies have an important gatekeeper function with respect to information access for voters (search engines and chatbots) as a communication channel between voters and parties (social media), and as a platform for discussion and the exchange of opinions (social media). AI-generated content, filtering and personalisation are helping to shape this information space. As a result, the Norwegian editor-controlled media face a more difficult competitive situation both financially, in terms of reaching users, and as an arena for public dialogue. In other words, the editor-controlled competitive arena includes not only social media such as Meta, X and TikTok, but also operators such OpenAI and Google as premise providers for the information landscape in connection with elections.

5.1.5 A more algorithm-driven distribution of content

While social media previously displayed content from users' personal networks, content is now increasingly determined by algorithms based on demographic characteristics and online activity—along with a growing share of content being promoted because platforms are paid to do so.

As noted above, this shift towards an algorithm-driven media is challenging both the information and the media landscape. As algorithms only expose users to content that supports their own opinions and perception of reality, this could contribute towards selective exposure. The way in which the information and media landscape in the United

¹³⁹ Veia, 2024

States works shows extreme examples of this, where voters in the two dominant parties do not read or listen to the same news or facts. Fortunately, this is not the case in Norway. It is also important to ensure a common public sphere where people can agree on basic facts and be presented with the same news and information sources even if they disagree on political positions.

Personalisation is not the sole challenge posed by an algorithm-driven distribution in the context of an election. An equally important challenge for the information landscape is that people are exposed to different content, and it is not guaranteed that others have been exposed to the same information as oneself. This makes public discourse more challenging, as personalisation puts pressure on two key democratic premises – the need for inclusive conversations as an arena for decision-making, and insight into the lives of others in order to make decisions for the common good.

The 2024 election year has also highlighted weaknesses of algorithm-driven social media as a source of information about politics and elections, such as the examples of YouTube’s recommendation algorithms in the Finnish presidential election and the type of content highlighted on TikTok during the European Parliament elections in Finland. Coupled with the fact that social media has increasingly deprioritised editorial content, it is becoming more difficult to reach people with quality-assured information.

5.2 Covert election influence

Prior to the *super election year*, there were significant concerns about what we might encounter with respect to influence operations and threat actors’ use of AI. Due to the nature of covert influence operations – in that they are carried out in a covert manner – it is not possible to determine the extent to which the actors have actually used AI. However, it is possible to draw some conclusions about how AI can enable actors to carry out such operations. With respect to covert influence operations, the Expert Group is of the opinion that the changes resulting from AI mainly involve the amplification of existing threats.

For a long time, it seemed that the election year would pass without any definitive proof that elections had been subjected to covert influence operations that could have altered the outcome. However, when the result of the presidential election in Romania was annulled on the grounds of foreign interference, the picture changed somewhat. The Expert Group believes Romania is an important example, not least because of the deliberate use of algorithm-driven social media, as well as cooperation between foreign and domestic actors in combination with cyber operations.

AI tools are rapidly evolving, but the key takeaway from 2024 is that the “traditional” methods of influence still appear to be just as important as new AI-based methods. This

does not imply that threat actors *are not* using AI. It must be assumed that the actors may have used 2024 to test and gain experience so that AI can contribute more heavily to future influence operations, primarily by streamlining and amplifying existing threats.

The Expert Group emphasises that there is still a strong need for more research-based knowledge about the importance of AI in the covert influence of elections.

In the following, we will mention specific changes to the problems of covert election influence:

5.2.1 Increased power and scale

It is the Expert Group's opinion that AI technology enables covert influence operations to gain greater power and scope. Greater power relates to the technology's capacity to scale up and produce more content to be included in the influence operation, whereas scope relates to AI reducing the need for human resources and finances to be able to carry out larger operations.

Examples of AI use in influence operations are the fake news websites that either present themselves as established media or as independent news websites, as we saw in the example of "D.C. Weekly". Fake websites are not a new phenomenon, even in Norway. In 2023, the Norwegian Defence Research Establishment found 14 fake websites purporting to be Norwegian. In reality, these sites were fraudulent and operated anonymously, using fabricated reporters with auto-copying and translating content from other sources.¹⁴⁰ Such websites can be automated using AI and distributed through fake social media profiles that may appear to be human, with tailored messages. The challenge when such sites and the distribution of their content become more sophisticated is that they can also become more widespread and persuasive. In the worst-case scenario, narratives spread from such sites may be quoted or repeated through editor-controlled media, which helps build false legitimacy.

5.2.2 A growing number of threat actors

Because AI reduces the resource requirements for influence operations, this poses the risk of existing threat actors such as Russia and China scaling up their efforts.¹⁴¹ At the same time, it can open the door for additional threat actors to enter the field and utilise methods that they previously did not have the resources or capacity to implement.

¹⁴⁰ Sivertsen, Lundberg, Albrechtsen, Dursun and Hegner, 2023

¹⁴¹ The Norwegian Police Security Service (PST), 2024

In the Expert Group's opinion, we must be prepared for the possibility that other state actors will use AI tools to conduct covert operations in connection with elections, and that this may include non-state actors both in Norway and in other countries. There is also a risk that companies will emerge seeking to profit from selling influence services, as with the Israeli company STOIC, which contributed to influence operations targeting the United States and Canada.¹⁴²

5.2.3 Increased personalisation of influence operations

Several of AI's possibilities can also be misused by threat actors as part of covert influence operations. One such problem is that threat actors can use AI to personalise and target their content to a greater extent, often down to the individual level.

One particular threat that has been highlighted is that AI enables the creation of bots with messaging services on social media that appear to be human and that establish one-to-one communication with users, such as on Snapchat or WhatsApp. German researcher Katja Muñoz pointed out such influence will be difficult to detect as the threat actor operates through direct messaging to individuals without leaving traces in open channels. She likens this to what influencers can achieve by establishing social and emotional relationships.¹⁴³

5.2.4 Increased polarisation and exploitation of divisive issues

A well-known strategy for influence operations is to use existing controversial issues or conflicts as a starting point and use these to further polarise and weaken trust in politicians and between people.¹⁴⁴ Such issues may include immigration, climate change, geographical differences, gender and foreign policy. If the message is triggering, it does not necessarily matter whether it is true, as long as the message supports and reinforces an existing point of view. AI offers greater power for operations that employ this, and it can be used to review large amounts of data to enable threat actors to form a better picture of issues that are likely to increase polarisation and weaken trust in society. This will be particularly relevant during elections.

¹⁴² Johnson, 2024

¹⁴³ Muñoz, 2024

¹⁴⁴ Bjørgul, Sivertsen and Sellevåg, 2022

5.2.5 Weakness in democratic preparedness that can be exploited

In order to make society less vulnerable to unwanted influences, it is also necessary for the population to have democratic preparedness. Therefore, the Expert Group believes it is particularly concerning that young people in Norway, despite their strong support for democratic values, are less likely to recognise threats to democracy. This may indicate a lower level of democratic preparedness.¹⁴⁵ If this preparedness is weakened, it could be exploited by threat actors.

Democratic preparedness is built over time, from the early school years. The media also plays a central role in this work. In Norway, democracy and good citizenship has been highlighted as an interdisciplinary topic in the new curricula from autumn 2020. This was an important step, supported by the Freedom of Expression Commission, which emphasised that the strengthening of democratic preparedness should primarily take place by further developing the infrastructure for freedom of expression.¹⁴⁶ The Expert Group shares the view that democratic preparedness for election influence operations should be included in other democracy lessons at school and not as an ad hoc measure. This requires that teachers have the necessary competence to adequately teach this subject.

Critical thinking is an important part of democratic preparedness.¹⁴⁷ This is a challenging duality. It is not enough to simply support democracy. Democracy must also be the subject of criticism in order to be further developed. Other actors play an important role in this work, such as non-governmental organisations, peace and human rights centres, as well as providers of educational resources and teaching materials.

5.3 The election process and cybersecurity

The Expert Group believes that lessons learnt from the 2024 elections are also transferable to the area of election process and cybersecurity. Further, the Expert Group believes that AI-facilitated changes to the election process and cybersecurity primarily involve the amplification of existing threats.

The authorities have long been aware of the possibility that Norwegian computer systems could be subject to cyberattacks and operations. Attacks or operations that

¹⁴⁵ Storstad, Caspersen and Wendelborg, 2023

¹⁴⁶ Official Norwegian Report (NOU) 2022: 9

¹⁴⁷ Børhaug, 2014

affect election processes could have major implications for both the practical conduct of the election and for its legitimacy and results.

The Expert Group points out that the massive scale of the cyber operation Romania was subjected to emphasises that foreign actors have both the capacity and ability to conduct large and coordinated operations. Even before 2024, there are examples of attacks on election authorities in the Nordic region, such as when the Swedish website for election results shut down as a result of a denial-of-service attack.

Denial-of-service attacks are the most commonly seen attacks targeting elections. Such attacks can undermine confidence in election process if they are successful in creating the impression that the systems have poor security. This is true even if such attacks do not achieve any significant changes to the systems or to the election outcome.

The Expert Group emphasises that there are elements of the Norwegian election process that contribute to a robust defence against cyberattacks and their possible impact on the election outcome. The most important element is that voting is done using paper ballots. This ensures that it is always possible to check and verify the correct results, even if the data system is attacked and disabled, or altered to produce false results.

In the United States, several people the Expert Group met with viewed the decentralised structure of elections as a strength. This makes it more difficult to actually influence the outcome. It would involve so many people that, in practice, it would be virtually impossible to implement such an attack without it becoming public knowledge. The practical implementation of elections is also decentralised in Norway and takes place in the municipalities.

Like Finland, Norway has extensive collaboration across authorities and areas of society. This strengthens the collective responsiveness and resilience throughout the entire electoral process, from pre-election planning to post-election implementation and follow-up. In both Finland and the United Kingdom, the importance of international cooperation was also highlighted.

In the following, the Expert Group will describe specific changes in the challenges involved in election processes and cybersecurity:

5.3.1 Increased digital vulnerability

Society is becoming increasingly digitised. This also applies to elections, where the EVA computer system supports the municipalities and county authorities in all phases of the election process.

The Expert Group believes that the service that publishes election results is particularly vulnerable to attack, and that attacks on this service could quickly impact confidence in the results, as seen with the attack on the Swedish Election Authority's website in 2018. If such incidents are not adequately handled, they can adversely impact confidence in both the conduct of the election and its results.

Cyber operations can influence elections even without affecting the actual systems used during the election. AI raises concerns about intrusions into systems where personal data and other information can be extracted and potentially spread online, as seen in the attack on Romanian computer systems, or sold to third parties. It is possible to manage this without AI, although AI-facilitated attacks will necessarily be more powerful.

With the personalisation capabilities inherent in AI, which were previously discussed as a challenge, threat actors can target intrusion attacks, particularly through more convincing phishing campaigns. Language models can also be trained on stolen material, which would enable them to create even more persuasive material that can be included in an influence operation.

In recent years, there have been several examples of cyberattacks on municipalities and government organisations, such as the attacks against Østre Toten Municipality in 2021¹⁴⁸ and, most recently, Gran Municipality in December 2024.¹⁴⁹ Even if such attacks do not directly affect the election and do not necessarily give attackers access to information or opportunities to make changes to the election administration system, incidents occurring during the election period will have a major impact on a municipality's capacity during an already resource-intensive period. Attacks against the central government, such as the widespread attacks against 12 government ministries in the summer of 2023¹⁵⁰, can put pressure on capacity or prevent national election authorities from doing their job. The Norwegian Parliament has also been exposed to cyberattacks several times.¹⁵¹ Such attacks can also contribute to weakening the general confidence that systems and data are adequately secured.

¹⁴⁸ Østby and Kowalski, 2022

¹⁴⁹ Gran Municipality, 2024

¹⁵⁰ Ministry of Local Government and Regional Development, 2023b

¹⁵¹ The Norwegian Police Security Service, 2020; Norwegian Parliament, 2021

5.3.2 Increased grounds for speculation about errors or fraud in the election process

Internationally, particularly in the United States, there has been a trend towards a diminished trust in elections over time. In the American context, it is particularly Republican voters who, over time, have developed less confidence in the election process. In the Expert Group's meetings, several people emphasised that there was a great deal of fabricated content that could have been used to discredit the election, and that a different election outcome would likely have changed its repercussions. Although Norway differs both in terms of its information and media landscape and in the actual conduct of its elections, it is problematic that international trends and debates could spill over into a Norwegian context, amplified by social media algorithms, and create false impressions of the situation in Norway. It is therefore essential for the election to be conducted in a way that does not give rise to such speculations.

Although AI also has the potential to improve and streamline election processes, the Expert Group is not familiar with any countries that have used AI in their actual conduct of elections, and the recommendations the Expert Group received indicates that we should show moderation. Several have pointed out that AI can be used to help identify errors for human follow-up, but not as an independent tool without supervision. Maintaining a paper-based system is also important to ensure verifiability and maintain confidence in the process and results.

Another impression the Expert Group would like to emphasise is the importance of ensuring that local election authorities have sufficient resources and expertise. Various actors the Expert Group spoke with in the United States mentioned that, over time, local election authorities have been given a growing number of tasks to manage.¹⁵² Due to the public's growing demands for information, they are increasingly expected to act as good communication advisors in addition to conducting a safe and efficient election.

It was therefore also noted that the role of the local election authorities must be defined, clarified and delimited. In Finland, the United Kingdom and the United States, election authorities emphasised that election authorities should not have the role of distinguishing between real and fake news, particularly with respect to politically controversial issues. Nor should they have to regulate the information space. The task of the election authorities must be to provide clear and correct information about the

¹⁵² Gorman and Levine, 2024

election and how it is conducted, and the information should primarily be presented on their own websites and through their own identifiable channels.

To avoid creating a breeding ground for speculation, it is essential to be transparent both during the actual conduct of the election and in the communication surrounding it. Elections are events where many people are involved, and some mistakes will be unavoidable. It is essential to have routines in place for managing this, as well as adequate communication. The Expert Group emphasises that the counting of ballots is a particularly critical phase where delays and errors in the transfer and publication of results can directly impact trust.

5.3.3 Gaps in AI expertise within public administration and politics

In the Expert Group's meeting with the political parties, it also became clear that there are major variations between the parties both in terms of their familiarity with AI and the extent to which they have employed AI tools in their own organisations.

For the authorities, it will be particularly important to ensure that they have the necessary expertise in AI tools to manage the changes and challenges it could entail. Central election authorities, such as the Norwegian Directorate of Elections, need to be well versed in the importance of AI in connection with elections and have sufficient resources to provide advice and guidance, for instance, to municipalities in the event incidents occur before, during or after an election.

6 Summarised assessments and recommendations by the Expert Group

AI has largely left its mark on the *super election year* of 2024. While there is no basis for concluding that AI has brought any groundbreaking new threats, it has left its mark on democracies and election processes. AI-generated content has been created and distributed, and in many cases, it has received widespread publicity. Thereby, AI has contributed to shaping election agendas. Social media based on algorithms, i.e. more “traditional” AI, has already had a major impact on the information and media landscape, and this also applies to elections. This has led to a new set of challenges for editor-controlled media as well as (election) authorities. Events and incidents during 2024 also indicate that cybersecurity in an election context has become even more crucial, which is particularly emphasised by the dramatic events during the presidential election in Romania, but also by events in the United States.

The Expert Group has assessed that AI contributes primarily to reinforcing existing threats. AI provides powerful tools that can simplify and streamline what previously required time, resources and expertise.

In a Norwegian context, the Expert Group believes that Norway is well-placed to prevent AI from adversely impacting Norwegian elections and the political discourse. This primarily involves resilience based on a significant degree of trust, as well as a diverse media landscape with strong editor-controlled media that appear to be highly aware of AI, elections and influence, and that can still reach large parts of the population. There are trends that are important to be aware of, particularly the media habits of young people. However, this also applies to other groups, such as immigrants and those who do not vote. Because these groups are less likely to use editorial media, it is essential to help them get accurate information about elections and to ensure that everyone knows where to find such information.

The Expert Group also emphasises the heavy dependence on foreign technology and platform companies, all of which are involved in the development of AI. This is a dependency that could have a major impact on the democratic foundation for elections in Norway. These companies wield great power over the infrastructure that controls the distribution of information, while there are few available alternatives.

The possibility of a decline in trust is the most serious consequence of the challenges identified by the Expert Group in Chapter 5. This applies to trust in the conduct and outcome of elections, as well as trust in the media and trust in information as such. The recommendations therefore emphasise measures that could contribute towards maintaining and building trust.

Based on our experience from the 2024 elections and other relevant research and knowledge in a Norwegian context, the Expert Group has arrived at recommendations on how the authorities can help mitigate the risk of AI having an adverse impact on elections and democracy.

In accordance with the mandate, several of the recommendations can be implemented before the parliamentary election in 2025. Several of the recommendations have a long-term perspective involving efforts to maintain and reinforce the structures that help to preserve a good information and media landscape and build resilience to unwanted influences.

It is not possible to isolate the efforts required and place them solely on election authorities or individual sectors. Efforts to mitigate the risk of adverse impacts on elections and democracy must be broad and involve a number of actors including election authorities, media authorities and the media themselves, security and digitalisation authorities, and not least, platform and technology companies. The Expert Group is therefore in favour of the existing interdepartmental working group and their efforts to build resilience against unwanted influence on elections, and is aware that the Expert Group's report will be considered by this group.

In conclusion, the Expert Group wishes to emphasise that the threat posed by AI should not be exaggerated. An exaggerated threat picture could itself result in diminished trust in information, technology, and democracy. Norway currently has a good foundation for resilience, which must be maintained and reinforced.

6.1 The Expert Group's recommendations

The Expert Group's recommendations will contribute to the following goals:

- Voters should have access to accurate information about elections.
- Ensure that the election process and digital systems that are important for elections are well protected.
- Safeguard and strengthen the Norwegian information and media landscape.
- Build resilience in the population and make us less vulnerable to unwanted election influence.

To achieve these goals, the Expert Group has the following recommendations:

- **Ensure that the electoral authorities possess the necessary competence and capacity in AI and communication.**

In a more ambiguous information landscape, it is even more important for election authorities to keep voters informed. Election authorities must be the main source of information about the election process. National election authorities, municipalities and county authorities must also have the necessary expertise and capacity. To contribute to this, the Expert Group notes the following:

- Election authorities must have sufficient resources, including resources working with communication to ensure more proactive information work.
- Develop expertise on AI and the impact it can have on elections among national election authorities, so that municipalities and county authorities can receive training and necessary guidance in this area.

- **Reduce the basis for speculation regarding errors and deficiencies in the election process or that the election is subject to unwanted influence.**

The Expert Group believes it is crucial for voters to have confidence that the election has been conducted properly and that the results are correct. The most important thing in order to achieve this is for the election to be conducted in accordance with legislation and international standards. Furthermore, the authorities must work to reduce the potential for speculation that the election has not been properly conducted. Therefore, the Expert Group recommends the following:

- Have backup solutions in place for important systems used in the conduct of elections, especially systems for communicating election results to the public. The backup solution should, as far as possible, be similar to the main solution.
- Continue using paper-based ballots to ensure verifiability.
- Be prepared to deal with misinformation and disinformation about election process. Prior to the election, procedures, and roles should be clarified so that national and local electoral authorities can help ensure that accurate information reaches the public.
- Intelligence and security services must have the necessary expertise and awareness of new challenges and threats to democracy due to AI.
- The authorities, including EOS services (the Parliament Appointed Committee for Intelligence Oversight), must endeavour to communicate as openly and quickly as possible, particularly about incidents or allegations of incidents that affect the election, in order to maintain trust.

- Recommendations by the Political Parties Act Committee on the revision of the Political Parties Act should be followed up to ensure transparency in the financing of election campaigns and political parties.
- Great caution should be exercised when implementing AI solutions in election administration.
- **Contact between the authorities and the technology and platform companies.**

Technology and platform companies have a great deal of power to determine how they organise their services, and the authorities should liaise with them on issues relating to election security. The Expert Group has noted certain areas of particular importance in such a dialogue:

- Labelling AI-generated content in accordance with the AI Act, provided the Act is not incorporated into Norwegian legislation prior to the parliamentary election.
 - Measures to prevent the spread of misinformation and disinformation about the election.
 - Platforms and chatbots should refer to official election information and exercise caution when discussing election-related matters.
 - Content from editor-controlled media should not be prevented in social media.
 - Clarify how the platforms can assist during incidents.
 - **Political actors should be held accountable and supported.**
- Political actors, including all those running for election, have an important responsibility to contribute to a good information landscape and avoid spreading misinformation or disinformation. At the same time, there should be measures in place to provide political actors with the necessary support and training, especially in the face of powerful platforms that can be difficult to get in touch with. The Expert Group would like to highlight the following:
- It is positive that an agreement has already been reached between the parties in the Norwegian Parliament to protect the 2025 parliamentary election from deepfakes and AI-generated disinformation. Such guidelines create a common framework across parties, and in the future, political actors should also look at the possibility of common guidelines for a broader consideration of AI.
 - Establish a point of contact for political parties and candidates to turn to in the event of incidents such as hacking or unauthorised removal of accounts, and to assist in the follow-up of platform companies.

- **Prioritise the rapid implementation of relevant EU legislation, especially the Digital Services Act and the AI Act.**

These laws provide important frameworks, including obligations for platforms to ensure openness and access, as well as requirements for labelling AI-generated content. Prioritising the implementation of these will be an important step in the regulation of technology and platform companies in Norway.

- **Pursue an active media policy that maintains an independent, strong and diverse editorial media landscape.**

The strong position of editor-controlled media must be maintained by ensuring that media policy will enable the media to be competitive and innovative in reaching more groups. As young people are increasingly using social media and chatbots as sources of information, it will be especially important to promote the use of editor-controlled media among the younger generations.

- **Develop source awareness and promote critical media, digital, and AI literacy skills.**

The public's ability to evaluate information and detect AI-generated misinformation and disinformation has become even more important given the opportunities provided by AI tools and with users moving from editor-controlled media to algorithm-driven social media. The Expert Group strongly recommends the following:

- Strengthen civil society organisations working to build greater source awareness and critical media literacy.
- The public must be informed of what unwanted election influence is, how it can happen and how they can detect it.
- It is essential for information initiatives to be aimed at groups that are less likely to use editor-controlled media.
- Easy-to-read and accessible material on AI and elections, based on knowledge from this report and other sources, should be made available for use in education when teaching lessons on democracy.

- **Increase research and cooperation between authorities, researchers, civil society and technology companies.**

Broad collaboration can ensure that technology is used responsibly and in line with democratic values, while simultaneously strengthening society's resilience to misuse. Such cooperation is also crucial for developing effective regulations and building trust in new solutions. The Expert Group therefore recommends the following:

- Provide more support for the research and knowledge sector to ensure that Norway has solid professional environments in areas of relevance for the topics in this report.
- Ensure that research is conducted on topics such as unwanted election influence, security, technology and international relations, technological infrastructure, source awareness and the critical understanding of media, technology, and AI.

- **International cooperation.**

The challenges identified extend beyond Norway's borders and challenge traditional international frameworks for international politics and rules of the road. The Expert Group therefore believes that Norway must be a driving force for international cooperation on issues related to AI, democracy and elections, as well as promoting a more ambitious technology policy globally to safeguard our democratic values and interests.

References

- Associated Press, (22 August 2024): *Company that sent fake Biden robocalls in New Hampshire agrees to \$1m fine*. Retrieved from The Guardian: <https://www.theguardian.com/technology/article/2024/aug/22/fake-biden-robocalls-fine-lingo-telecom>
- Bakke, S. (16 December 2024): *For første gang er et demokratisk valg annullert på grunn av cyberoperasjoner* [For the first time, a democratic election has been cancelled due to cyber operations] Retrieved from digi.no: <https://www.digi.no/artikler/debatt-for-forste-gang-er-et-demokratisk-valg-annullert-pa-grunn-av-cyberoperasjoner/554014>
- Baste, Ø. F., Schultz, A. and Osberg, J. A. (18 October 2023): *Mens vi venter på at EU skal regulere kunstig intelligens* [While we're waiting for the EU to regulate artificial intelligence]. *Stat & Styring*, pp. 15-20. doi:10.18261/stat.33.3.3
- Bekkengen, F. V. (2024): *The Norwegian media barometer 2023*. Statistics Norway. Retrieved from <https://www.ssb.no/kultur-og-fritid/tids-og-mediebruk/artikler/norsk-mediebarometer-2023>
- Bergh, J., Christensen, D. A. and Holmås, T. H. (2021): *Mobiliseringsvalget 2019: Hadde kommunereformen noen betydning?* [The mobilisation election 2019: Did the municipal reform have any effect?] I J. Saglie, S. B. Seggaard and D. A. Christensen (ed.): *Lokalvalget 2019. Nye kommuner – nye valg?* [The 2019 Local Elections. New municipalities – New choices?] Cappelen Damm Akademisk.
- Bergh, J., Christensen, D. A and Holmås, T.-H. (2023): *Valgdeltakelse, forhåndsstemmegivning og familiens betydning for politisk deltakelse* [Voter turnout, advance voting and the significance of family for political participation]. I J. Bergh and A. H. Haugsgjerd (ed.): *Politikk i urolige tider. En studie av stortingsvalget 2021* [Politics in uncertain times. A study of the 2021 parliamentary election].
- Bjørgul, L., Sivertsen, E. G. and Sellevåg, S. R. (2022): *Scenarioer for uønsket påvirkning i forbindelse med norske valg* [Scenarios for unwanted influence in connection with Norwegian elections]. The Norwegian Defence Research Establishment. Retrieved from <https://www.ffi.no/publikasjoner/arkiv/scenarioer-for-uonsket-pavirkning-i-forbindelse-med-norske-valg>
- Blenkinsop, P. (17 December 2024): *EU opens investigation into TikTok over election interference*. Retrieved from Reuters: <https://www.reuters.com/business/eu-opens-investigation-into-tiktok-over-election-interference-2024-12-17/>

- Brandtzæg, B. A., Magnussen, E., Vike, H., Heian, M. T., Kvernenes, M. S., Jupskås, A. R. and Ruud, S. S. (2022). *Lokaldemokrati og lokalpolitikernes arbeidsvilkår. Motivasjon og deltakelse i lokalpolitisk arbeid* [Local democracy and local politicians' working conditions. Motivation and participation in local political work]. Telemark Research Institute. Retrieved from https://www.regjeringen.no/contentassets/a1de937bf67a44dda49f1f95ab9a0c92/sluttrapport_lokaldemokrati_tf.pdf
- Brautović, M. and Roško, M. (2024): *Generative AI Use and disinformation during the Croatian parliament elections 2024*. Adria Digital Media Observatory. Retrieved from https://edmo.eu/wp-content/uploads/2024/06/ADMO_report_8.pdf
- Børhaug, K. (2014): Selective Critical Thinking: A Textbook Analysis of Education for Critical Thinking in Norwegian Social Studies. *Policy Futures in Education*, pp. 431-444. doi:10.2304/pfie.2014.12.3.431
- Caspersen, J., Wendelborg, C. and Storstad, O. (2023). *Ett steg fram og to tilbake: Demokratiforståelse, holdninger og deltakelse blant norske ungdomsskoleelever* [One step forward, two steps back: Understanding of democracy, attitudes, and participation among Norwegian lower-secondary school pupils]. NTNU Social Research. Retrieved from <https://samforsk.no/publikasjoner/ett-steg-fram-og-to-tilbake-demokratiforstaelse-holdninger-og-deltakelse-blant-norske-ungdomsskoleelever>
- Châtelet, V. (11 June 2024a): *Far-right parties employed generative AI ahead of European Parliament elections*. Retrieved from DFRLab: <https://dfrlab.org/2024/06/11/far-right-parties-employed-generative-ai-ahead-of-european-parliament-elections/>
- Châtelet, V. (4 July 2024b): *Operation targets French snap elections using AI-generated content*. Retrieved from DFRLab: <https://dfrlab.org/2024/07/04/operation-targets-french-snap-elections-using-ai-generated-content/>
- CheckFirst (2024): *Ads, Influence, and Democracy: Meta's Role in Romania's 2024 Presidential Election*. CheckFirst. Retrieved from https://checkfirst.network/wp-content/uploads/2024/12/Research%20Note%20Ads,%20Influence,%20and%20Democracy_%20Meta%E2%80%99s%20Role%20in%20Romania%E2%80%99s%20Election.pdf
- Chesney, B. and Citron, D. (2019): Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, pp. 1753-1820. doi:10.15779/Z38RV0D15J

- Coldewey, D. (12 November 2024): *Generative disinfo is real — you're just not the target, warns deepfake tracking nonprofit*. Retrieved from TechCrunch: <https://techcrunch.com/2024/11/12/generative-disinfo-is-real-youre-just-not-the-target-warns-deepfake-tracking-nonprofit/>
- Connal, S. (2024): *Providing more data about news results in the EU*. Retrieved from Google: <https://blog.google/around-the-globe/google-europe/more-data-about-news-results-eu/>
- Cybersecurity and Infrastructure Security Agency (2024): *Election Security*. Retrieved from Cybersecurity and Infrastructure Security Agency: <https://www.cisa.gov/topics/election-security>
- Dahlum, S., Langsæther, P. E. and Wig, T. (2 November 2024): *Også norske velgere kan støtte en autoritær leder* [Norwegian voters could support an authoritarian leader]. Retrieved from vg.no: <https://www.vg.no/nyheter/i/KMG014/norske-statsvitere-ogsaa-i-norge-er-den-autoritaere-trusselen-reell>
- DGA Group (2024): *AI and Elections: Impact and implications of AI generated content*. DGA Group. Retrieved from <https://dgagroup.com/insight/ai-and-elections-impact-and-implications-ai-generated-content/>
- Ministry of Digitalisation and Public Governance, 3 September 2021): *EUs forslag til regulering av KI - Norges posisjon* [The EU's proposal for AI regulation – Norway's position] Retrieved from Regjeringen.no: <https://www.regjeringen.no/no/tema/statlig-forvaltning/it-politikk/KI-strategi/nasjonal-posisjon-pa-ki-regulering/id2870299/>
- Ministry of Digitalisation and Public Governance (n.d.): *Ny forordning for kunstig intelligens* [New act on artificial intelligence]. Retrieved from Digdir.no: <https://www.digdir.no/kunstig-intelligens/ny-forordning-kunstig-intelligens/4271>
- The Norwegian Agency for Public and Financial Management (DFØ) (2024): *Innbyggerundersøkelsen 2024* [Citizen Satisfaction with Public Services Survey 2024]. Retrieved from dfo.no: <https://dfo.no/undersokelser/innbyggerundersokelsen-2024>
- Economist Intelligence, 2024 *Democracy Index 2023. Age of conflict*. Economist Intelligence. Retrieved from <https://www.eiu.com/n/campaigns/democracy-index-2023/>
- EEAS (2024): *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*. European Union External Action. Retrieved from

https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

Elliott, V. (29 May 2024a): *Germany's Far-Right Party Is Running Hateful Ads on Facebook and Instagram*. Retrieved from WIRED: <https://www.wired.com/story/meta-racist-ads-germany-eu-elections/>

Elliott, V. (11 June 2024b): *There's an AI Candidate Running for Parliament in the UK*. Retrieved from WIRED: <https://www.wired.com/story/ai-candidate-running-for-parliament-uk/>

EU DisinfoLab, 2024: *What is the Doppelganger operation? List of resources*. Retrieved from EU DisinfoLab: <https://www.disinfo.eu/doppelganger-operation/>

European Board of Digital Services (2024): *Report on the European Elections Digital Services Act and Code of Practice on Disinformation*. European Union. Retrieved from <https://digital-strategy.ec.europa.eu/en/library/european-board-digital-services-publishes-post-election-report-eu-elections>

European Commission (16 June 2022): *Signatories of the 2022 Strengthened Code of Practice on Disinformation*. Retrieved from European Commission: <https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation>

European Commission (2024): *Memo: Known information interference operations during the June 2024 elections for the European Parliament*. European Commission. Retrieved from commission.europa.eu: <https://ec.europa.eu/commission/presscorner/api/files/attachment/879707/Memo%20-%20Known%20information%20interference%20operations%20during%20EP%20elections.pdf>

European Parliament (2024a): *How European elections work*. Retrieved from European Parliament: <https://elections.europa.eu/en/how-elections-work/>

European Parliament (2024b): *European elections: EU institutions prepared to counter disinformation*. Retrieved from European Parliament: <https://www.europarl.europa.eu/news/en/press-room/20240603IPR21804/european-elections-eu-institutions-prepared-to-counter-disinformation>

EUvsDisinfo (19 June 2024): *Doppelganger Strikes Back: Unveiling FIMI Activities Targeting European Parliament Elections*. Retrieved from EUvsDisinfo:

<https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/>

EØS-notatbasen [EEA Note Database] (19 November 2024a): *Digital Services Act - DSA*. Retrieved from Regjeringen.no: <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/forordning-om-digitale-tjenester-digital-services-act-dsa/id2860429/>

EØS-notatbasen [EEA Note Database]. (10 June 2024b): *European Media Freedom Act - EMFA*. Retrieved from Regjeringen.no: <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2022/nov/forordning-om-mediefrihet-european-media-freedom-act-emfa/id2950946/>

Goldmacher, S. (11 August 2024): *Trump Falsely Claims That the Crowds Seen at Harris Rallies Are Fake*. Retrieved from The New York Times: <https://www.nytimes.com/2024/08/11/us/politics/trump-harris-crowds-ai.html>

Gorman, L. and Levine, D. (2024): *The ASD AI Election Security Handbook*. GMF Alliance for Securing Democracy. Retrieved from <https://www.gmfus.org/news/asd-ai-election-security-handbook>

Gotfredsen, S. G. (12 September 2024): *The Tenet Media Incident*. Retrieved from Columbia Journalism Review: https://www.cjr.org/the_media_today/tenet_media_indictment_russia.php

GOV.uk (28 October 2024): *UK sanctions Putin's interference actors*. Retrieved from GOV.uk: <https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors>

Gran Municipality (18 December 2024): *Gran kommune er utsatt for dataangrep* [Gran Municipality subjected to cyberattack]. Retrieved from Gran Municipality: <https://www.gran.kommune.no/gran-kommune-er-utsatt-for-dataangrep.6701579-452652.html>

Gundersen, M. (19 February 2019): *Slik kan den nye etterretningsloven påvirke deg* [How the new Intelligence Service Act could affect you]. Retrieved from NRKbeta: <https://nrkbeta.no/2019/02/14/slik-kan-den-nye-etterretningsloven-pavirke-deg/>

Haugsgjerd, A. H., Karlsen, R. and Aalberg, T. (2023): *Nyhetsbruk og politisk kunnskap i valgkamp* [News consumption and political knowledge in election campaigns]. I J. Bergh and A. H. Haugsgjerd (ed.): *Politikk i urolige tider. En studie av stortingsvalget 2021* [Politics in uncertain times. A study of the 2021 parliamentary election]. Oslo: Cappelen Damm Akademisk.

- Haugsgjerd, A. and Karlsen, R. (2022): Election Campaigns, News Consumption Gaps, and Social Media: Equalizing Political News Use When It Matters? *The International Journal of Press/Politics*, 29(2). doi:10.1177/19401612221112014
- Haugsgjerd, A. and Seggaard, S. B. (2020): *Politisk tillit, lokaldemokrati og legitimitet. Kunnskapsstatus og utviklingstrekk* [Political trust, local democracy and legitimacy. Knowledge status and development trends]. The Institute for Social Research. Retrieved from <https://hdl.handle.net/11250/2652187>
- Heggheim, S. and Sællmann, S. K. (5 July 2023): *Laga falsk nettside om politisk parti* [Made fake website about political party]. Retrieved from NRK.no: <https://www.nrk.no/sorlandet/laga-falsk-nettside-om-politisk-parti-1.16469868>
- Hofsrud, Ø. (13 June 2024): *Google får konkurranse som søkefavoritt – nå går de unge til TikTok og ChatGPT* [Google receives competition as preferred search engine – young people now use TikTok and ChatGPT]. Retrieved from Kampanje.com: <https://kampanje.com/premium/juni-2024/innsikt/google-far-konkurranse-som-sokefavoritt-na-gar-de-unge-til-tiktok-og-chatgpt>
- Hogan Lovells (15 July 2024): *France prohibits non-consensual deep fakes*. Retrieved from Hogan Lovells: <https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes>
- Hudnall, H. (2024): *Image of Donald Trump wading through flood water is AI-generated | Fact check*. Retrieved from USA Today: <https://eu.usatoday.com/story/news/factcheck/2024/10/03/ai-image-trump-hurricane-helene-fact-check/75483588007/>
- IKT-Norge (26 November 2024): *Enighet om å beskytte stortingsvalget mot deepfakes. IKT-Norge samlet de politiske partiene om avtale*. [Agreement to protect the parliamentary election against deepfakes. ICT-Norway got the political parties to coalesce around agreement]. Retrieved from IKT-Norge: <https://ikt-norge.no/meninger/enighet-om-a-beskytte-stortingsvalget-mot-deepfakes-ikt-norge-samlet-de-politiske-partiene-om-avtale/>
- Independent High Level Expert Group set up by the European Commission (2018): *A Definition of AI: Main Capabilities and Disciplines*. Retrieved from <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>
- International IDEA (2024): *Code of Conduct for the 2024 European Parliament Elections*. Retrieved from International IDEA: <https://www.idea.int/european-code-of-conduct-2024>

- International Society for Fair Elections and Democracy (2024): *First Interim Report on Social Media Monitoring. August 27 - September 20*. ISFED. Retrieved from <https://www.isfed.ge/eng/sotsialuri-mediis-monitoringi/sotsialuri-mediis-monitoringis-pirveli-shualeduri-angarishi-27-agvisto-20-seqtemberi>
- Ipsos (2023): *Hatytringer, trusler og desinformasjon mot folkevalgte* [Hate speech, threats, and disinformation against elected officials]. Ipsos for the Norwegian Association of Local and Regional Authorities (KS). Retrieved from <https://www.ks.no/globalassets/fagomrader/forskning-og-utvikling/fou-rapporter/Hatytringer-trusler-og-desinformasjon-mot-folkevalgte.pdf>
- Jackson, D., Weil, M. and Adler, W. T. (2024): *Preparing for Artificial Intelligence and Other Challenges to Election Administration*. Bipartisan Policy Center. Retrieved from <https://bipartisanpolicy.org/report/preparing-for-artificial-intelligence-and-other-challenges-to-election-administration/>
- Jerijervi, D. R. and Hauger, K. K. (15 June 2023): *Slår alarm om ny Facebook-trend: - Bekymrer meg veldig* [Alarm bells sounded over new Facebook trend: "Very concerning".] Retrieved from Kampanje.com: <https://kampanje.com/premium/juni-2023/innsikt/ny-facebook-trend-vekker-uro-i-medie-norge---bekymrer-meg-veldig/>
- Johnson, D. B. (5 June 2024): *Israeli influence operation highlights global disinformation industry*. Retrieved from CyberScoop: <https://cyberscoop.com/israel-influence-operations-stoic/>
- Kalsnes, B. and Ihebæk, K. A. (2021): *Hva vet vi egentlig om medievalgkampen?* [What do we really know about the media election campaign?] *Norsk medietidsskrift* [Norwegian Media Journal], 28(3), pp. 1-2. doi:10.18261/ISSN.0805-9535-2021-03-01
- Karlsen, R. (in publication): Chapter 17: Election Campaigns. In *Oxford Handbook of Norwegian Politics*.
- Karlsen, R. and Steen-Johansen, K. (2021): *Nyheter, sosiale nettverk og lokalpolitisk orientering i lokalvalgkamp* [News, social networks and local political orientation in local elections] I J. Saglie, S. B. Segard and D. A. Christensen (ed.): *Lokalvalget 2019. Nye kommuner – nye valg?* [The 2019 Local Elections. New municipalities – New choices?] Oslo: Cappelen Damm Akademisk.
- Katzenberger, T. (10 February 2024): *Judge blocks California deepfakes law that spared Musk-Newsom row*. Retrieved from POLITICO:

<https://www.politico.com/news/2024/10/02/california-law-block-political-deepfakes-00182277>

Kleven, Ø. (8 November 2023): *Nær halvparten av velgerne stemte på forhånd* [Nearly half of all voters cast their ballots in advance]. Retrieved from [ssb.no: https://www.ssb.no/valg/kommunestyre-og-fylkestingsvalg/statistikk/valgresultat-for-kommunestyre-og-fylkestingsvalget/artikler/naer-halvparten-av-velgerne-stemte-pa-forhand](https://www.ssb.no/valg/kommunestyre-og-fylkestingsvalg/statistikk/valgresultat-for-kommunestyre-og-fylkestingsvalget/artikler/naer-halvparten-av-velgerne-stemte-pa-forhand)

Kleven, Ø. and Bergseteren, T. (2024): *Velgerundersøkelsen 2023. Tabellrapport*. [2023 Election Survey. Report of tables]. Statistics Norway. Retrieved from <https://www.ssb.no/valg/kommunestyre-og-fylkestingsvalg/artikler/velgerundersokelsen-2023.tabellrapport>

Knutsen, C. H., Dahlum, S., Allern, E. H., Hagfors, S. B., Klausen, J. E., Søyland, M. and Wig, T. (2023): *Tilstandsanalyse av det norske demokratiet* [Report on the status of Norwegian Democracy]. Universitetet i Oslo. Retrieved from <https://www.regjeringen.no/no/dokumenter/tilstandsanalyse-av-det-norske-demokratiet/id2991191/>

Knuutila, A. and Havula, P. (2024): *The TikTok Effect. How the app shaped political discourse during Finnish European elections 2024*. Fact bar. Retrieved from <https://crossover.social/wp-content/uploads/2024/07/TheTiktokEffect.pdf>

Knuutila, A., Kuster, G. and Lesplingart, A. (2024): *“Up Next”, biased politics? YouTube Recommendations and Political Bias in the Finnish Presidential Election 2024*. Fact bar. Retrieved from https://crossover.social/wp-content/uploads/2024/03/Digitaalivahti_raportti_2024.pdf

Ministry of Local Government and Regional Development, (9 June 2023a): *Regjeringa lanserer tiltaksplan for å sikre valet* [The Government launches action plan to secure the election]. Retrieved from [Regjeringen.no: https://www.regjeringen.no/no/aktuelt/regjeringa-lanserer-tiltaksplan-for-a-sikre-valet/id2983730/](https://www.regjeringen.no/no/aktuelt/regjeringa-lanserer-tiltaksplan-for-a-sikre-valet/id2983730/)

Ministry of Local Government and Regional Development, (24 July 2023b): *Departementer utsatt for dataangrep* [Government ministries subjected to cyberattacks]. Retrieved from [Regjeringen.no: https://www.regjeringen.no/no/aktuelt/presseinvitasjon/id2990098/](https://www.regjeringen.no/no/aktuelt/presseinvitasjon/id2990098/)

Linvill, D. and Warren, P. (2023): *Infektion's Evolution: Digital Technologies and Narrative Laundering*. Clemson University Media Forensics Hub. Retrieved from https://open.clemson.edu/mfh_reports/3/

- LSM (9 May 2024): *Deep-fake use to influence elections will be criminalized in Latvia*. Retrieved from LSM.lv: <https://eng.lsm.lv/article/politics/election/09.05.2024-deep-fake-use-to-influence-elections-will-be-criminalized-in-latvia.a553370/>
- Lüders, M. and Sundet, C. S. (3 October 2022): *Globalt innfødte som en tapt generasjon? En konseptualisering av unge som en mediegenerasjon* [Globally native as a lost generation? Conceptualisation of young people as a media generation]. *Norsk medietidsskrift*, pp. 1-12. doi:10.18261/nmt.30.1.1
- Marinov, V. (23 May 2024): *Don't Bother Asking AI About the EU Elections: How Chatbots Fail When It Comes to Politics*. Retrieved from Correctiv: <https://correctiv.org/en/fact-checking-en/2024/05/23/dont-bother-asking-ai-about-the-eu-elections-how-chatbots-fail-when-it-comes-to-politics/>
- Matza, M. (23 January 2024): *Fake Biden robocall tells voters to skip New Hampshire primary election*. Retrieved from BBC News: <https://www.bbc.com/news/world-us-canada-68064247>
- The Norwegian Media Authority, 2023 *Mediemangfaldsrekneskapen 2022. Mediemangfald i eit bruksperspektiv*. [2022 Media Diversity Accounts. Media diversity from a user perspective]. The Norwegian Media Authority. Retrieved from https://www.medietilsynet.no/globalassets/publikasjoner/mediemangfoldsregnskap/230327_bruksmangfald_2023.pdf
- The Norwegian Media Authority, (2024a): *Norsk medieøkonomi 2019–2023. Ein rapport om den økonomiske utviklinga i norske medieverksemder*. [Norwegian Media Economics 2019–2023. Report on economic developments in Norwegian media companies]. The Norwegian Media Authority. Retrieved from https://www.medietilsynet.no/globalassets/publikasjoner/medieokonomi/241024_medieokonomi_2019-2023.pdf
- The Norwegian Media Authority (10 October 2024b): *Kritisk medieforståelse i den norske befolkningen 2024* [Critical media literacy in the Norwegian population 2024]. Retrieved from Medietilsynet: <https://www.medietilsynet.no/fakta/rapporter/kritisk-medieforstaelse/rapporter-2024/kmf2024/>
- The Norwegian Media Authority, (2024c): *De globale plattformenes etterlevelse av bransjenormen mot desinformasjon* [Global platforms' compliance with industry standards against disinformation]. The Norwegian Media Authority. Retrieved from https://www.medietilsynet.no/globalassets/publikasjoner/bransjenorm-desinfo/240909_plattformenes_etterlevelse_bransjenormen_desinformasjon.pdf

- Meyer-Resende, M., Davis, A., Denkovski, O. and Allen, D. (2024): *Are Chatbots Misinforming Us About the European Elections? Yes*. Democracy Reporting International. Retrieved from <https://democracy-reporting.org/en/office/global/publications/chatbot-audit>
- Moe, H. and Bjørgan, J. (2024): *Bruksmønstre for digitale nyheter 2024* [Patterns of use for digital news 2024]. Reuters Digital News Report Norge. Retrieved from <https://frittord.no/attachments/ecd0cca9e62c496298df2e13d3efb0c26fa6e279/358-20240617064556955390.pdf>
- Moe, H. and Bjørgan, J. (2024): *Nyheter og kunstig intelligens* [News and artificial intelligence]. Retrieved from Reuters Digital Report Norway: <https://nyhetsbruk.w.uib.no/rapport-2024/nyheter-og-kunstig-intelligens/>
- Munich Security Conference (2024): *A Tech Accord to Combat Deceptive Use of AI in 2024 Elections*. Retrieved from Munich Security Conference: <https://securityconference.org/en/aielectionsaccord/>
- Muñoz, K. (2024): *The AI Election Year: How to Counter the Impact of Artificial Intelligence*. German Council on Foreign Relations e. V. Retrieved from https://dgap.org/system/files/article_pdfs/DGAP-MEMO-Nr-1-2024_EN.pdf
- Norwegian National Security Authority (2024): *Risiko 2024* [Risk 2024]. Norwegian National Security Authority Retrieved from [nsm.no: https://nsm.no/getfile.php/1313477-1719434219/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf](https://nsm.no/getfile.php/1313477-1719434219/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf)
- Nehamas, N., Schleifer, T. and Corasaniti, N. (10 September 2024): *Taylor Swift Endorses Kamala Harris*. Retrieved from The New York Times: <https://www.nytimes.com/2024/09/10/us/taylor-swift-endorses-kamala-harris.html>
- Newman, C. (1. July 2024): *Exclusive: Top UK politicians victims of deepfake pornography*. Retrieved from Channel 4 News: <https://www.channel4.com/news/exclusive-top-uk-politicians-victims-of-deepfake-pornography>
- Newman, N., Fletcher, R., Robertson, C., Arguedas, A. and Nielsen, R. (2024): *Reuters Institute Digital News Report 2024*. Reuters Institute for the Study of Journalism. Retrieved from https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf
- The Norwegian Human Rights Institution and the Norwegian Board of Technology, (2023): *Generativ kunstig intelligens og ytringsfrihet* [Generative artificial intelligence and freedom of expression]. The Norwegian Human Rights Institution and the

- Norwegian Board of Technology. Retrieved from <https://media.wpd.digital/teknologiradet/uploads/2023/12/Generativ-kunstig-intelligens-og-ytringsfrihet-DIGITAL.pdf>
- Official Norwegian Report (NOU) 2020: 6 *Frie og hemmelige valg. Ny valglov* [Free and secret elections — New Election Act]
- Official Norwegian Report (NOU) 2022: 9 National strategy for an open and informed public discourse.
- Official Norwegian Report (NOU) 2023: 17 *Nå er det alvor. Rustet for en usikker fremtid* [This is serious – Prepared for an uncertain future].
- Olari, V. (12 December 2024): *Rise of unknown Romanian presidential candidate preceded by Telegram and TikTok engagement spikes*. Retrieved from DFRLab: <https://dfrlab.org/2024/12/12/romania-candidate-telegram-tiktok/>
- Olsen, R. K., Kalsnes, B. and Barland, J. (2024): Do Small Streams Make a Big River? Detailing the Diversification of Revenue Streams in Newspapers' Transition to Digital Journalism Businesses. *Digital Journalism*, 12. doi:10.1080/21670811.2021.1973905
- OpenAI (30 May 2024): *AI and Covert Influence Operations: Latest Trends*. OpenAI. Retrieved from Disrupting deceptive uses of AI by covert influence operations: https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcc18b633/Threat_Intel_Report.pdf
- Oslo Economics and Norwegian Computing Centre (2023): *Knowledge acquisition on electronic and internet-based solutions for voting*. Oslo Economics. Retrieved from <https://www.regjeringen.no/contentassets/f7c349a901bf49598a4f28cbb4a8d5c/oe-rapport-118-kunnskapsinnhenting-e-valg.pdf>
- The Political Parties Act Committee (18 December 2023): *Partiloven: Reformbehov Brev fra Partilovnemnda til statsråd Erling Sande* [The Political Parties Act: Needs for reform. Letter from the Political Parties Act Committee to Minister Erling Sande]. Retrieved from https://www.partilovnemnda.no/contentassets/dd3a9ba9f66c43acb20d8d90df7e3a75/brev-statsrad-reformbehov_.pdf
- The Norwegian Police Security Service (2024): *National Threat Assessment 2024*. The Norwegian Police Security Service. Retrieved from https://www.pst.no/globalassets/2024/nasjonal-trusselvurdering-2024/nasjonal-trusselvurdering-2024_uuweb.pdf

- The Norwegian Police Security Service (8 December 2020): *Datainnbruddet mot Stortinget er ferdig etterforsket*. Retrieved from pst.no: <https://www.pst.no/alle-arterikler/pressemedlinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/>
- Prop. 45 (Bill) (2022–2023) Act relating to parliamentary and local government elections (Election Act)
- Raj, S. (18 April 2024): *How A.I. Tools Could Change India's Elections*. Retrieved from The New York Times: <https://www.nytimes.com/2024/04/18/world/asia/india-election-ai.html>
- Reuters (18 December 2024): *Romanian parliament sees evidence of election meddling, committee says*. Retrieved from Reuters: <https://www.reuters.com/world/europe/romanian-parliament-sees-evidence-election-meddling-committee-says-2024-12-18/>
- Rybalka, M. (25 September 2024): *7 av 10 unge bruker KI* [7 out of 10 young people use AI]. Retrieved from Statistics Norway: <https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/bruk-av-ikt-i-husholdningene/artikler/7-av-10-unge-bruker-ki>
- Scholl, M. v. (27 August 2024): *So hilft den Parteien KI im Wahlkampf* [How AI aids parties in election campaigns] Retrieved from ZDF Heute: <https://www.zdf.de/nachrichten/politik/deutschland/ki-kuenstliche-intelligenz-landtagswahl-parteien-100.html>
- Schueler, M., Romano, S., Stanusch, N., Çetin, R. B., Tabti, S., Faddoul, M. and Lilley, I. (2024): *Artificial Elections - Exposing the Use of Generative AI Imagery in the Political Campaigns of the 2024 French Elections*. AI Forensics. Retrieved from <https://aiforensics.org/work/french-elections-2024>
- Scott, M. (7 May 2024): *Moldova fights to free itself from Russia's AI-powered disinformation machine*. Retrieved from POLITICO: <https://www.politico.eu/article/moldova-fights-free-from-russia-ai-power-disinformation-machine-maia-sandu/>
- Simon, F., Fletcher, R. and Nielsen, R. K. (2024): *How generative AI chatbots responded to questions and fact-checks about the 2024 UK general election*. Reuters Institute. doi:10.60625/risj-c4vm-e367
- Sivertsen, E. G., Bjørgul, L., Lundberg, H., Endestad, I., Bornakke, T., Kristensen, J. B., Christensen, N. M. and Albrechtsen, T. (2021): *Unwanted foreign influence? Analysis of the Norwegian parliamentary elections 2021*. The Norwegian Defence Research Establishment. Retrieved from <https://www.ffi.no/publikasjoner/arkiv/uonsket-utenlandsk-pavirkning-kartlegging-og-analyse-av-stortingsvalget-2021>

- Sivertsen, E. G., Lundberg, H., Albrechtsen, T., Dursun, A. and Hegner, S. (2023): *Two layers of fog - anonymous Norwegian websites linking to Russian-affiliated domains*. The Norwegian Defence Research Establishment. Retrieved from <https://www.ffi.no/publikasjoner/arkiv/two-layers-of-fog-anonymous-norwegian-websites-linking-to-russian-affiliated-domains>
- Sjøvaag, H., Ferrer-Conill, R. and Olsen, R. K. (2024): Capture Beyond the Platforms: The Material and Infrastructural Conditions for Digital Journalism. *Digital Journalism*, pp. 1-20. doi:10.1080/21670811.2024.2377078
- Sjøvaag, H., Olsen, R. K. and Ferrer-Conill, R. (2024): Delivering content: Modular broadcasting technology and the role of content delivery networks. *Telecommunications Policy*. Retrieved from <https://hdl.handle.net/11250/3165378>
- Skjuve, M., Brandtzaeg, P. B. and Følstad, A. (2024): Why do people use ChatGPT? Exploring user motivations for generative conversational AI. *First Monday*, 29(1). doi:10.5210/fm.v29i1.13541
- Solheim, Ø. B. and Enjolras, B. (2023): *Notat om nordmenns bruk av kunstig intelligens* [Memo on Norwegians' use of artificial intelligence]. The Centre for Research on Civil Society and Voluntary Sector. Retrieved from <https://www.samfunnsforskning.no/aktuelt/nyheter/2023/notat-om-nordmenns-bruk-av-kunstig-intelligens---solheim-og-enjolras---isf.pdf>
- Spring, M. (13 February 2023): *Sadiq Khan says fake AI audio of him nearly led to serious disorder*. Retrieved from BBC: <https://www.bbc.com/news/uk-68146053>
- Stocking, G., Wang, L., Lipka, M., Matsa, K. E., Widjaya, R., Tomasik, E. and Liedke, J. (2024): *America's News Influencers. The creators and consumers in the world of news and information on social media*. Pew Research Center. Retrieved from https://www.pewresearch.org/wp-content/uploads/sites/20/2024/11/PJ_2024.11.18_news-influencers_report.pdf
- Stockwell, S. (2024): *AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections*. The Alan Turing Institute Centre for Emerging Technology and Security. Retrieved from <https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-threat-analysis-2024-uk-and-european-elections>
- Stockwell, S., Hughes, M., Swatton, P. and Bishop, K. (2024): *AI-Enabled Influence Operations: Threat to the UK General Election*. The Alan Turing Institute Centre for Emerging Technology and Security. Retrieved from <https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-threat-uk-general-election>

- Storstad, O., Caspersen, J. and Wendelborg, C. (2023): *Ett steg fram og to tilbake. Demokratiforståelse, holdninger og deltakelse blant norske ungdomsskoleelever* [One step forward, two steps back: Understanding of democracy, attitudes, and participation among Norwegian lower-secondary school pupils]. Norwegian University of Science and Technology (NTNU). Retrieved from https://samforsk.no/uploads/files/NTNU-samf_IEA-rapport.pdf
- The Storting (10 March 2021): *Stortinget utsatt for IT-angrep* [The Storting subjected to cyberattack]. Retrieved from Stortinget.no: <https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2020-2021/stortinget-utsatt-for-it-angrep/>
- The Constitutional Court of Romania, 6 December 2024): *Press Release, 6 December 2024*. Retrieved from The Constitutional Court of Romania: <https://www.ccr.ro/en/press-release-6-dec/>
- United Nations AI Advisory Body (2024): *Governing AI for Humanity. Final Report*. United Nations. Retrieved from https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf
- United States Election Assistance Commission, 7 June 2023): *Help America Vote Act*. Retrieved from United States Election Assistance Commission: https://www.eac.gov/about/help_america_vote_act.aspx
- United States Election Assistance Commission, (2024): *Artificial Intelligence (AI) and Election Administration*. Retrieved from United States Election Assistance Commission: <https://www.eac.gov/AI>
- Vallgård, P. (24 May 2019): *Attacken mot Valmyndighetens sajt polisanmäldes – förundersökningen lades ned* [The attack on the Swedish Election Authority's website was reported to the police – the preliminary investigation was closed]. Retrieved from Sveriges Radio: <https://sverigesradio.se/artikel/7228619>
- The Swedish Election Authority (n.d.): *Vårt IT-stöd* [Our IT support]. Retrieved 13 December 2024 from <https://www.val.se/om-oss/vart-uppdrag/vart-it-stod.html>
- V-Dem Institute (2024): *Democracy Report 2024: Democracy Winning and Losing at the Ballot*. University of Gothenburg. Retrieved from <https://www.v-dem.net/publications/democracy-reports/>
- Veia, I. K. (14 October 2024): *Meta har stengt HL-senterets Facebook-side. Beslutningen er endelig* [Meta has closed the Norwegian Centre for Holocaust and Minority Studies' Facebook page. The decision is final]. Retrieved from Aftenposten:

<https://www.aftenposten.no/meninger/debatt/i/8qRPgW/meta-tar-rollen-som-ytringsfrihetens-portvokter-kan-samfunnet-leve-med-det>

Verma, P., Oremus, W. and Zakrzewski, C. (9 November 2024): *AI didn't sway the election, but it deepened the partisan divide*. Retrieved from The Washington Post: <https://www.washingtonpost.com/technology/2024/11/09/ai-deepfakes-us-election/>

Vigdor, 2024 (19 August 2024): *Trump Promotes A.I. Images to Falsely Suggest Taylor Swift Endorsed Him*. Retrieved from The New York Times: <https://www.nytimes.com/2024/08/19/us/politics/trump-taylor-swift-ai-images.html>

Williams, A. (17 June 2024): *AI-generated image of Keir Starmer shared to suggest Labour no longer represents the working class*. Retrieved from Logically Facts: <https://www.logicallyfacts.com/en/fact-check/fake-ai-generated-image-of-keir-starmer-shared-to-suggest-labour-no-longer-represents-the-working-class>

Wong, J. C. (12 January 2018): *Facebook overhauls News Feed in favor of 'meaningful social interactions'*. Retrieved from The Guardian: <https://www.theguardian.com/technology/2018/jan/11/facebook-news-feed-algorithm-overhaul-mark-zuckerberg>

World Economic Forum (10 January 2024): *Global Risks Report 2024*. Retrieved from World Economic Forum: <https://www.weforum.org/publications/global-risks-report-2024/>

Zhuang, Y. (11 February 2024): *Imran Khan's 'Victory Speech' From Jail Shows A.I.'s Peril and Promise*. Retrieved from The New York Times: <https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html>

Østby, G. and Kowalski, S. J. (2022): *Hendelseshåndtering ved cyberangrepet mot Østre Toten kommune. Hva kan vi lære av håndteringen?* [Incident response during the cyberattack on Østre Toten Municipality. What can we learn from the response?] Norwegian University of Science and Technology (NTNU). Retrieved from https://www.ototen.no/_f/p1/idbd37a14-f91f-41e5-9fa2-14977f2a7977/v-10-ostre-toten.pdf

Appendix 1: Overview of whom the Expert Group met with and received input from

The Expert Group has held input meetings and received written input from various actors, including authority organisations, media actors, civil society and others.

Below is an overview of those who provided input to the Expert Group's work at meetings and on our journeys respectively (in alphabetical order):

Input provided at meetings

- Arbeiderpartiet (The Labour Party)
- AUF (Workers' Youth League)
- Faktisk.no
- Fremskrittspartiet (The Progress Party)
- Google
- Høyre (The Conservative Party)
- Kristelig folkeparti (The Christian Democratic Party)
- The Ministry of Culture and Equality
- Mediebedriftenes Landsforening – MBL (The Norwegian Media Businesses' Association)
- Medietilsynet (The Norwegian Media Authority)
- Meta
- Miljøpartiet De Grønne (The Green Party)
- The Psychological Defence Agency (MPF, Sweden)
- The Norwegian National Security Authority (NSM)
- Norsk Journalistlag (The Norwegian Union of Journalists)
- Norsk Presseforbund (The Norwegian Press Association)
- Norsk Redaktørforening (The Association of Norwegian Editors)
- The Norwegian Broadcasting Corporation (NRK)
- OSCE Office for Democratic Institutions and Human Rights (ODIHR)
- The Norwegian Police Security Service (PST)
- Rødt (The Red Party)
- Senter for kildebevissthet (Centre for Source Awareness)
- Senterpartiet (The Centre Party)
- Senterungdommen (Centre Youth)
- SimulaMet
- Snapchat
- Sosialistisk Ungdom (Socialist Youth)
- Teknologirådet (The Norwegian Board of Technology)

- TikTok
- The Election Research Programme at the Norwegian Institute for Social Research
- Venstre (The Liberal Party)
- VG

Input during study visits

- Alan Turing Institute, Centre for Emerging Technology and Security (CETaS)
- Atlantic Council, Digital Forensic Research Lab
- Axios
- Bipartisan Policy Center
- Cybersecurity and Infrastructure Security Agency (CISA)
- Directorate-General for Communications Networks, Content and Technology (DG Connect), Brussel
- Election Observation and Democracy Support (EODS), Brussels
- EU Election Unit
- European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), Helsinki
- European External Action Service (EEAS), Brussels
- Georgetown University, Center for Security and Emerging Technology (CSET)
- George Washington University, School of Media & Public Affairs
- German Marshall Fund US
- The Ministry of Justice in Finland
- Microsoft
- National Association of State Election Directors (United States)
- National Cyber Security Centre (NCSC), United Kingdom
- NATO
- Nordic Press Center
- Royal Norwegian Embassy in Helsinki (Finland)
- Royal Norwegian Embassy in London (United Kingdom)
- Royal Norwegian Embassy in Washington D.C. (United States)
- Mission of Norway to the European Union, Brussels
- R Street Institute
- Shoutout UK
- State Board of Elections in Maryland
- UK Electoral Commission
- University of Helsinki
- United States Election Assistance Commission

Written input from Norwegian foreign and permanent missions/delegations

Requests were sent on behalf of the Expert Group to all Norwegian foreign and permanent missions/delegations for contributions and any experiences gain from the countries they follow, which could be of relevance for the group's work. This written input has been used as the foundation for the Expert Group's work.

The following Norwegian foreign and permanent missions/delegations provided written input (in alphabetical order):

- Royal Norwegian Embassy in Abuja (Nigeria)
- Royal Norwegian Embassy in Berlin (Germany)
- Royal Norwegian Embassy in Budapest (Hungary)
- Royal Norwegian Embassy in Canberra (Australia)
- Royal Norwegian Embassy in Islamabad (Pakistan)
- Royal Norwegian Embassy in Copenhagen (Denmark)
- Royal Norwegian Embassy in Madrid (Spain)
- Royal Norwegian Embassy in Paris (France)
- Royal Norwegian Embassy in Rome (Italy)
- Royal Norwegian Embassy in Seoul (South Korea)
- Royal Norwegian Embassy in Singapore (Singapore)
- Royal Norwegian Embassy in Stockholm (Sweden)
- Royal Norwegian Embassy in Warsaw (Poland)
- Royal Norwegian Embassy in Zagreb (Croatia)
- Mission of Norway to the European Union, Brussels
- Permanent Mission of Norway to the United Nations Office and other international organizations, Geneva
- The Permanent Delegation of Norway to the OSCE, Geneva

Published by:

The Expert Group for AI and Elections,
appointed by the Ministry of Local Government and Regional Development

Ordering of publications:

The Norwegian Government Security and Service Organisation
publikasjoner.dep.no

Telephone: 22 24 00 00

Publications are also accessible at:

www.regjeringen.no

Publication code: H-2563

Cover photo/illustration: iStock