



**Regulating Manipulative Political Bots Around Political Elections:
The Artificial Intelligence Act and the Charter of Fundamental Rights of
the European Union**

Gizem YARDIMCI

Student Number: 21252157

Thesis submitted in partial fulfilment for the Degree of Doctor of Philosophy Maynooth
University, School of Law and Criminology

Date: 29 October 2025

Head of Department: Professor Fergus Ryan
Supervisor: Dr David MANGAN

Dedication

Dedicated to Mustafa Kemal Atatürk's ideal of a democratic, secular and modern Republic of Turkey.

İlelebet, payidar.

Acknowledgement

I would like to thank my supervisor, Dr David Mangan, for his guidance, support, patience and kindness in this process. This was a challenging journey for me, and without Dr Mangan's encouragement and support, this thesis would not have been possible to complete. I am deeply grateful for his open communication, his constant support, and the clarity with which he shared his advice; thus, I always felt I was in safe hands.

This research was funded by Research Ireland from 2021-2025. This financial support allowed me to undertake this research, participate in international conferences, contribute to research networks and disseminate my findings. I thank Research Ireland, the Centre for Advanced Networks for Sustainable Societies (ADVANCE CRT), Professor Deirdre Desmond and all my peers in ADVANCE CRT for always being supportive.

Many thanks to each of the participants in this doctoral study for sharing their knowledge and experience so generously and for giving of their time.

I sincerely thank the School of Law and Criminology at Maynooth University, its inspiring academics and my peers for providing a healthy academic environment and making me feel part of a supportive community. In particular, I appreciate the Director of Postgraduate Research Programmes of the School of Law and Criminology at Maynooth University, Professor Delia Ferri, for her open communication and support.

I am also grateful for Dr Maria Helen Murphy. At the very beginning of this study, Dr Murphy made this PhD opportunity possible for me, for which I am grateful, and shared valuable comments and feedback on early versions of my thesis.

I would like to thank Professor Aphra Kerr for her guidance in ensuring that this research, with its interdisciplinary nature and interview components, met the ethical requirements of Maynooth University.

Many thanks to Helen Kirrane for her kindness, support and friendship, and to Matthew McKenna for his friendship, our inspiring weekly walks, and for generously sharing his experiences of the PhD process.

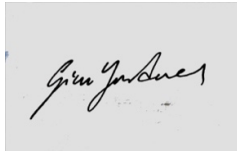
To Altuğ Yalçıntaş — my academic mentor and my co-author. A true intellectual companion and collaborator, whose guidance, patience, and mentorship have been invaluable throughout this journey.

To Emre Özbaş — my partner in life, my *elocan*. Thank you for standing by my side through every stage of this PhD journey and for your unwavering support.

Plagiarism Declaration

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of PhD in Law and Criminology, is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed:

A handwritten signature in black ink, appearing to read "Gini Jones", is written on a light gray rectangular background.

Date: 29 October 2025

Table of Contents

DEDICATION	2
ACKNOWLEDGEMENT.....	3
PLAGIARISM DECLARATION	4
TABLE OF CONTENTS	5
ABSTRACT.....	8
LIST OF FIGURES	9
LIST OF KEY ABBREVIATIONS.....	10
CHAPTER 1: INTRODUCTION.....	11
<i>1.1. Context of Thesis.....</i>	<i>11</i>
1.1.1. Political Bots in the Age of AI.....	11
1.1.2. Scope of the Research.....	22
1.1.3. What is a Bot?.....	24
1.1.4. What are Political Bots?.....	30
<i>1.2. Methodology of Thesis: A Socio-Legal Analysis of Political Bots</i>	<i>41</i>
1.2.1. Research Purpose	44
1.2.2. Research Questions.....	45
1.2.3. Methodology	46
1.2.3.1. Qualitative Research Methodology.....	46
1.2.3.2 Socio-legal Research Model	49
1.2.3.3. Other Methodologies Considered	51
1.2.4. Procedures for Data Capture.....	51
1.2.4.1. Document Analysis.....	51
1.2.4.2. Interviewing and Transcription.....	52
1.2.5. Conclusion	54
<i>1.3. Structure of Thesis</i>	<i>55</i>
<i>1.4. Conclusion</i>	<i>59</i>
CHAPTER 2: THEORETICAL FRAMEWORK: POLITICAL BOTS AND THE CHANGING POLITICAL PUBLIC SPHERE	61
2.1. INTRODUCTION: THEORETICAL FRAMEWORK	61
2.2. POLITICAL BOTS AND THE CHANGING POLITICAL PUBLIC SPHERE	63
2.2.1. <i>The Position of Political Bots in the Public Sphere.....</i>	<i>63</i>
2.2.2. <i>Are Political Bots the Digital Continuation of Traditional Media in Electoral Campaigns?</i>	<i>69</i>
2.2.3. <i>As Digitalization Transforms Media, What Is the Role of Political Bots in New Media?</i>	<i>81</i>
2.3. MEDIATION AND AUTOMATION OF POLITICAL COMMUNICATION	93
2.3.1. <i>The Evolution of Political Communication and Influence on Electoral Campaigns</i>	<i>94</i>
2.3.2. <i>Platforms' Responsibilities from the Perspective of Political Bots.....</i>	<i>95</i>
2.3.3. <i>Can Automation Enhance the Efficiency of Computational Propaganda?</i>	<i>98</i>
2.4. GOVERNANCE OF POLITICAL BOTS AROUND ELECTIONS.....	101
2.5. CONCLUSION.....	112

CHAPTER 3: LEGAL FRAMEWORK IN THE AI ACT FOR POLITICAL BOTS .114

3.1. INTRODUCTION.....	114
3.2. HOW DOES THE AI ACT REGULATE POLITICAL BOTS?	115
3.2.1. <i>Are Political Bots Within the Scope of the AI Act?</i>	117
3.2.2. <i>Risk-based Categorisation of Political Bots Under the AI Act</i>	121
3.2.2.1. Political Bots as High-Risk AI Systems	124
3.2.2.2. Generative AI-Driven Political Bots and GPAI.....	133
3.2.2.3. FRIA for Political Bots	138
3.2.3. <i>Specific Regulatory Dimensions Applicable to Political Bots</i>	141
3.2.3.1. Mimicking Human Users.....	141
3.2.3.2. Interaction with Natural Persons.....	144
3.2.3.3. Spreading AI-Generated Content.....	146
3.2. THE REFLECTION OF THE DSA ON POLITICAL BOTS	149
3.3. COULD THE CFR PROVIDE FURTHER PROTECTION AGAINST POLITICAL BOTS?	155
3.3.1. <i>Political Bots and Freedom of Expression</i>	157
3.3.2. <i>Interrelation of Political Bots with Other Rights Under the CFR</i>	166
3.3.2.1. Article 7 and Article 8 of the CFR.....	166
3.3.2.2. Article 39 of the CFR.....	169
3.4. CONCLUSION.....	172

CHAPTER 4: ANALYSIS OF INTERVIEW DATA.....175

4.1. OVERVIEW	175
4.2. INTERVIEWING PROCESS	176
4.2.1. <i>Interviewing</i>	176
4.2.2. <i>Demographic Reflections on Interviews</i>	180
4.2.3. <i>Transcription</i>	185
4.3. ETHICAL CONSIDERATIONS	186
4.3.1 <i>Ethical Approval</i>	186
4.3.2 <i>Confidentiality and Anonymity</i>	187
4.3.3 <i>Informed Consent</i>	188
4.4. DATA ANALYSIS	189
4.4.1 <i>Data Analysis Software</i>	190
4.4.2 <i>Coding and Memos</i>	191
4.5. RESEARCH INTEGRITY, TRUSTWORTHINESS AND LIMITATIONS.....	192
4.5.1 <i>Research Design and Limitations</i>	194
4.5.2. <i>Trustworthiness</i>	197
4.5.3. <i>Research Implications</i>	198
4.6. THEME DEVELOPMENT FOR MAXQDA ANALYSIS.....	199
4.6.1. <i>AI Systems</i>	201
4.6.2. <i>Bots</i>	207
4.6.2.1. Bot Description	207
4.6.2.2. Bots in Perspective: Understanding Risks and Responses	213
4.6.2.3. Bots in the Political Sphere.....	219
4.6.2.3.1. Supportive Perspectives on the Use of Bots in the Public Sphere.....	220
4.6.2.3.2. Critical Perspectives on the Use of Bots in the Public Sphere	222
4.6.2.3.3. Practical Pathways for Bot Governance	225
4.6.2.4. Effectiveness of Existing Legal Frameworks in Governing Political Bot Usage.....	226
4.6.3. <i>Democracy</i>	229
4.6.3.1. Democracy: An Overview	229

4.6.3.2. The Media Environment in the Age of Political Bots.....	232
4.6.3.3. Platform Responsibility in Relation to the Functions of Political Bots	236
4.6.4. <i>Ethics</i>	239
4.6.5. <i>Governance</i>	243
4.6.5.1. General Approaches of the Participants.....	243
4.6.5.2. Challenges in the Regulation Process of the AI Act and Their Underlying Dynamics	247
4.6.6. <i>Discussion</i>	249
4.6.7. <i>Future Research</i>	254
4.7. CONCLUSION.....	255
CHAPTER 5: CONCLUSION	257
5.1. INTRODUCTION.....	257
5.2. RESEARCH OVERVIEW	258
5.3. LIMITATIONS	261
5.4. KEY CONCLUSIONS, RECOMMENDATIONS, AND FUTURE RESEARCH	262
5.4.1. <i>Key Conclusions</i>	263
5.4.2. <i>Recommendations</i>	268
5.4.3. <i>Future Research</i>	272
5.5. CONCLUDING COMMENT.....	273
BIBLIOGRAPHY	275
APPENDICES	306
ANNEX I - INTERVIEW INFORMATION SHEET	306
ANNEX II - ETHICAL APPROVAL	312
ANNEX III - INTERVIEW QUESTIONS FOR SG1	313
ANNEX IV - INTERVIEW QUESTIONS FOR SG2.....	315
ANNEX V- INTERVIEW QUESTIONS FOR SG3	317
ANNEX VI - CODE SYSTEM	319
ANNEX VII - DOCUMENT SYSTEM.....	320
ANNEX VIII - DETAILED CODE SYSTEM	321
ANNEX IX - MEMOS.....	326

Abstract

The question of how political bots impact freedom of expression and information, and conversely, how these rights apply to political bots themselves remain a contested issue. This is because political bots are used to drive engagement metrics to other bots, in particular political bots. They are commonly used in artificial intelligence (AI) embedded systems. Today, Twitterbots are perhaps the most well-known type of political bot including bots on Telegram, Facebook Messenger, Discord, Slack, WhatsApp and Instagram, and have been used for their impact on political elections. The threat posed by political bots has been identified in many cases, such as the 2016 US election and the 2016 BREXIT referendum. But, this threat has also been observed in democratic processes across Europe, including in France and Germany in 2017, in Sweden in 2022, and in Croatia in 2024. Such bots have been employed to effectively execute various organised activities, ranging from disinformation campaigns and candidate discrediting to the generation of echo chambers on platforms and the impairment of access to accurate information. Across various disciplines, including media studies, political communication, sociology and political science, the effects of political bots on elections have been studied; however, this effect has not been proven certain. Nevertheless, the reaction of the European Union (EU) currently relies on two main documents: the European Union Code of Practice on Disinformation and the AI Act (Regulation (EU) 2024/1689). This PhD project asks two main research questions: (1) How are political bots used as a tool for manipulation in political elections in Europe? (2) How could the European Union's AI Act regulate the use of political bots as tools for manipulation without interfering with pluralism and freedom of expression and information? Therefore, this research aims to present a detailed socio-legal analysis of the potential influence of the EU's AI Act on political bots from the perspective of freedom of expression and information (as articulated in Article 11 of the Charter of Fundamental Rights of the European Union). Additionally, the research relies on Habermas's public sphere theory. Thus, a socio-legal research methodology and qualitative research methodology are used for a 'law in context' analysis, and semi-structured interviews have been conducted with experts from a range of disciplines.

Key words: political bots, AI Act, democracy, political campaigns, information.

List of Figures

<i>Figure 1. Overview of SG1.</i>	181
<i>Figure 2 : Overview of SG2.</i>	182
<i>Figure 3 : Overview of SG3.</i>	184
<i>Figure 4. Experience of interviewees.</i>	185
<i>Figure 5. Word cloud of the most frequent words used in all interviews.</i>	200
<i>Figure 6. Overview of frequency of main themes referenced by interviewees.</i>	201
<i>Figure 7. Most frequent words to define AI.</i>	202
<i>Figure 8. This word cloud reflects the frequently used words.</i>	202
<i>Figure 9. The co-occurrence of words used by interviewees.</i>	203
<i>Figure 10. Definitions of AI as provided by interviewees.</i>	204
<i>Figure 11. Descriptions about bots provided by interviewees.</i>	213

List of Key Abbreviations

AI	Artificial Intelligence
AI Act	Artificial Intelligence Act
AI-HLEG	Artificial Intelligence High Level Expert Group
AI Office	The European AI Office
CEO	Chief Executive Officer
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DSA	Digital Service Act
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation
GPT	Generative Pre-trained Transformers
GPAI	General-Purpose AI
LLMs	Large Language Models
MAXQDA	A computer-assisted qualitative data analysis software
MIT	Massachusetts Institute of Technology
NGO	Non-governmental Organisation
NLG	Natural Language Generation
NLP	Natural Language Processing
NLU	Natural Language Understanding
SG1	Subgroup 1
SG2	Subgroup 2
SG3	Subgroup 3
TTPA	Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising
US	United States

Chapter 1: INTRODUCTION

1.1.Context of Thesis

1.1.1. Political Bots in the Age of AI

Increased Interaction, Greater Access to Information, and Growing Fragility in Democracy

Digital tools have significantly expanded the interaction with democratic participation, particularly through online platforms that facilitate campaigning, deliberation, and mobilization. However, the audience in the digital sphere is not always composed of real people. For instance, bots —automated programs that mimic human interaction— are increasingly used in political arena for various purposes, often with significant implications for the integrity, security, and trustworthiness of democratic processes. Moreover, this phenomenon in the political arena emerged recently compared to their use in the commercial context.¹ The interactions of bots with society produce both positive and negative effects, depending on their intended use.

Bots typically use natural language to engage in conversational interaction,² perform task automation,³ make autonomous decisions⁴ and reasoning.⁵ They are internet-based

¹ Madeline Lamo and Ryan Calo, ‘Regulating Bot Speech’ (2019) 66 UCLA Law Review 988, 997.

² See Carlene Lebeuf, Margaret-Anne Storey and Alexey Zagalsky, ‘Software Bots’ (2018) 35 IEEE Software 18, 19 <<https://doi.org/10.1109/MS.2017.4541027>>. In Section 1.1.3, “What is a Bot?”, it is also explained that advanced chatbots leverage natural language processing (NLP) and large language models to understand user intent, maintain context, and generate human-like responses.

³ One of the oldest and most fundamental bot capabilities is automating repetitive, tedious tasks. It is noted that even before bots became widely used for political purposes, they were primarily employed to perform tasks that people found monotonous, did not enjoy, or could not complete quickly. Nick Monaco and Samuel C Woolley, *Bots* (Polity Press 2022) s 1.

⁴ In the gaming industries, non-player character (NPC) bots are common, and they can use AI to make tactical decisions, adapt to player strategies, and simulate intelligent behaviour in real time. See more Georgios N Yannakakis and Julian Togelius, *Artificial Intelligence and Games* (Springer International Publishing 2018) 38 <<https://doi.org/10.1007/978-3-319-63519-4>> accessed 1 May 2026.

⁵ In software engineering, bots can triage bugs, review code, and run integration or performance tests, interpret test results and decide on deployment pipelines without human intervention. See Linda Erlenhov, Francisco

applications.⁶ Also, bots conduct information retrieval and synthesis,⁷ manage social media and create content.⁸ Some bots can monitor systems, services, or data streams and send alerts when thresholds are exceeded or anomalies are detected.⁹ Bots also enable personalisation and adaptation by learning user preferences over time and tailoring interactions accordingly.¹⁰

In the early days, bots were solely software applications that ran automated or repetitive tasks. Nevertheless, their relatively primitive characteristics were sufficient to enable their use for malicious purposes. For instance, they were employed as tools in political campaigns,¹¹

Gomes De Oliveira Neto and Philipp Leitner, 'An Empirical Study of Bots in Software Development: Characteristics and Challenges from a Practitioner's Perspective' *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (ACM 2020) 445 and 449 <<https://doi.org/10.1145/3368089.3409680>> accessed 1 May 2026.

⁶ As Orabi and others highlight, since bots can create and exchange user-generated content, they are considered internet-based applications. They function as automated accounts in an online social network. So, the notion of a social network is based on the definition provided by Kaplan and Haenlein, who define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content." See Mariam Orabi and others, 'Detection of Bots in Social Media: A Systematic Review' (2020) 57 *Information Processing & Management* 102250, 1 <<https://doi.org/10.1016/j.ipm.2020.102250>>; Andreas M Kaplan and Michael Haenlein, 'Users of the World, Unite! The Challenges and Opportunities of Social Media' (2010) 53 *Business Horizons* 59, 61 <<https://doi.org/10.1016/j.bushor.2009.09.003>>.

⁷ For example, they carried out maintenance tasks and formed the backbone of search engines such as Google, Yandex, and Bing, as they were responsible for gathering and organising information. Monaco and Woolley (n 3) s 1.

⁸ Bots can autonomously post content, and they can like, retweet, follow, or unfollow accounts. They also interact with other users on social media platforms. Thus, such bots serve for marketing or community management purposes of commercial institutions. See details about Retweet Bots Tuğrulcan Elmas, Rebekah Overdorf and Karl Aberer, 'Characterizing Retweet Bots: The Case of Black Market Accounts' (2022) 16 *Proceedings of the International AAAI Conference on Web and Social Media* 171, 171 <<https://doi.org/10.1609/icwsm.v16i1.19282>>.

⁹ For software development, bots monitor build statuses and notify teams regarding failures in the system. Chatbots can also be used in healthcare systems. For instance, they can support conversational interviewing with stroke survivors to monitor patients after discharge. See Lebeuf, Storey and Zagalsky (n 2) 20; Milo M Skovfoged and others, 'Supporting Understanding: Comparing Conversational Interviewing in Chatbot vs Human-Administered Patient-Reported Outcomes for Stroke Survivors' [2026] *ACM Transactions on Computing for Healthcare* 3799983, 16 <<https://doi.org/10.1145/3799983>>.

¹⁰ E-commerce chatbots recommend products based on browsing history. Also, OpenAI released that they will start serving ads in the free version of their chatbot.

See Manik Rakhra and others, 'E-Commerce Assistance with a Smart Chatbot Using Artificial Intelligence' *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)* (IEEE 2021) 145 <<https://doi.org/10.1109/ICIEM51511.2021.9445316>> accessed 1 May 2026; Cade Metz, 'OpenAI Starts Testing Ads in ChatGPT' *The New York Times* <<https://www.nytimes.com/2026/01/16/technology/chatgpt-ads-openai.html>>.

¹¹ Bello Shehu Bello and Reiko Heckel, 'Analyzing the Behaviour of Twitter Bots in Post Brexit Politics' *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (IEEE 2019) <<https://doi.org/10.1109/SNAMS.2019.8931874>> accessed 5 September 2023.

targeting different spectrums of the audiences based on their profiles.¹² In some cases, bots could create echo chambers that limit individuals' exposure to diverse perspectives. Moreover, bots contributed to the creation of an environment shaped by misinformation, disinformation, and micro-targeting. This is why, voters might encounter only a narrow range of views on social media, potentially leading them to feel isolated in their opinions¹³ and even pressuring them to reconsider their initial opinions or their support of a candidate.

In addition, nowadays, bots can interfere in candidate selection processes within political parties. For example, bots can be used to spread claims that a candidate has left their party, or to disseminate other allegations reflecting internal power struggles within political parties.¹⁴ This way, manipulation can target not just voters but also influence political parties to reposition their electoral strategies. Additionally, this bot-driven manipulation can influence the real-time interactions between specific voter groups.

Political bots have also contributed positively to certain aspects of democratic processes. Thanks to bot-driven interaction, candidates' popularity boosts in elections.¹⁵ The impact of

¹² Jacob Ratkiewicz and others, 'Truthy: Mapping the Spread of Astroturf in Microblog Streams' *Proceedings of the 20th international conference companion on World wide web* (ACM 2011)

<<https://doi.org/10.1145/1963192.1963301>> accessed 31 August 2023; Linda Risso, 'Harvesting Your Soul? Cambridge Analytica and Brexit' *Brexit Means Brexit?* (Akademie der Wissenschaften und der Literatur 2018).

¹³ Felix M Simon, "'We Power Democracy': Exploring the Promises of the Political Data Analytics Industry' (2019) 35 *The Information Society* 158, 11 <<https://doi.org/10.1080/01972243.2019.1582570>>.

¹⁴ For instance, in Turkey, the Victory Party (Zafer Partisi) became a key strategic actor in the presidential elections of 2023. The party and their candidate, Sinan Oğan, gained popularity primarily through social media. In particular, Sinan Oğan became the focus point of disinformation campaigns. Allegations about Oğan's resignation—which, in reality, did not occur—along with other unfounded assertions were spreading as misinformation campaigns. These examples reveal how misinformation strategies can exploit both inter-party rivalries and struggle for control within party structures. See Seden Akcinaroglu and others, 'An Exploration of the Influence of Misinformation and Detering Technologies' (2023) 4 <https://www.cmu.edu/ideas-social-cybersecurity/events/ideas2023_paper_8501.pdf>; Tobias R Keller and Ulrike Klinger, 'Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications' (2019) 36 *Political Communication* 171, 3 <<https://doi.org/10.1080/10584609.2018.1526238>>.

¹⁵ Iva Nenadić, 'Unpacking the "European Approach" to Tackling Challenges of Disinformation and Political Manipulation' (2019) 8 *Internet Policy Review* 5 <<https://doi.org/10.14763/2019.4.1436>> accessed 19 October 2025.

bots on public opinion and voting behaviour can also be visible in election results. Moreover, the use of digital tools during democratic processes can cause predictions about election results to fluctuate, making social media visibility critical for candidates until the very last moment of the elections.¹⁶ The most well-known example of this was observed during the 2016 presidential race between Hillary Clinton and Donald Trump.¹⁷ According to Allcott and Gentzkow, Donald Trump would not have been elected president were it not for the influence of fake news in 2016.¹⁸ Political bots played a key role in the spread of fake news.¹⁹

On the other hand, research by Bessi and Ferrara shows that Trump's supporters seem significantly more positive than Clinton's supporters, regardless of whether the source is human or bot.²⁰ Indeed, this electoral period overlapped with political bot activity, which reached an all-time high during 2016 election in the US.²¹ Most importantly, pro-Trump campaigners and programmers carefully adjusted the timing of content production during the debates. As a result, the increasing pace of automated pro-Trump activity over time might have influenced the electoral result. In addition, the widening gap between highly automated pro-Trump and pro-Clinton activity also appears to have been significant. During the first debate,

¹⁶ Sarah Grevy Gotfredsen, 'Harris Is Outspending Trump on Social Media. How Much Does That Matter?' Columbia Journalism Review (24 October 2024)

<https://www.cjr.org/the_media_today/harris_trump_social_media_ads_meta_google.php>.

¹⁷ Alessandro Bessi and Emilio Ferrara, 'Social Bots Distort the 2016 U.S. Presidential Election Online Discussion' [2016] First Monday <<https://firstmonday.org/ojs/index.php/fm/article/view/7090>> accessed 1 September 2023; Also, the research has examined the extent to which online traffic patterns before and after the televised debates between Clinton and Trump in 2016 may have affected the election results. See Bence Kollanyi, Philip N Howard and Samuel C Woolley, 'Bots and Automation over Twitter during the Third U.S. Presidential Debate' [2016] COMPROP DATA MEMO 2016.3 / 27 OCT 2016 <<https://demtech.oii.ox.ac.uk/research/posts/bots-and-automation-over-twitter-during-the-third-u-s-presidential-debate/>>.

¹⁸ Hunt Allcott and Matthew Gentzkow, 'Social Media and Fake News in the 2016 Election' (2017) 31 Journal of Economic Perspectives 211, 211 <<https://doi.org/10.1257/jep.31.2.211>>.

¹⁹ Chengcheng Shao and others, 'The Spread of Low-Credibility Content by Social Bots' (2018) 9 Nature Communications 4787, 11 <<https://doi.org/10.1038/s41467-018-06930-7>>.

²⁰ Bessi and Ferrara (n 17) 8.

²¹ Bence Kollanyi, Philip N. Howard and Samuel C Woolley, 'Bots and Automation over Twitter during the U.S. Election' (2016) 2016.4 <<https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2016/11/Data-Memo-US-Election.pdf>>.

there were four pro-Trump tweets for every single pro-Clinton tweet (a 4:1 ratio), whereas by election day, this had grown to five to one (5:1).²²

Moreover, alongside the United States, political bots influence, and continue to influence elections across the Europe. In 2012, bots were identified as being used for political purposes, including artificially increasing follower counts, amplifying engagement (e.g., likes), and constructing perceptions of popularity.²³ However, what begins as limited bot activity has been developed into a force that shapes electoral processes over time. For instance, during the 2017 German parliamentary election, bot activity on German Twitter was observed to be operating in the service of the far-right Alternative für Deutschland (AfD).²⁴ In 2024, the German government released a report showing that the 2025 Bundestag elections could be targeted by a pro-Russian disinformation campaign involving a bot army.²⁵

In Czechia, intelligence reports have identified coordinated TikTok bot activity and manipulation to support anti-system parties in Czech elections.²⁶ A TikTok-driven campaign involving bots was also observed during the 2024 presidential elections in Romania.²⁷

²² *ibid* 4.

²³ Andrea Vogt, 'Hot or Bot? Italian Professor Casts Doubt on Politician's Twitter Popularity' *The Guardian* (Milan, 22 July 2012) <<https://doi.org/https://www.theguardian.com/world/2012/jul/22/bot-italian-politician-twitter-grillo>>.

²⁴ AfD entered parliament for the first time in 2017. By 2026, the party appears to have reached a record level of support of 28%, according to polls. Lisa-Maria Neudert, Bence Kollanyi and Philip N. Howard, 'Junk News and Bots during the German Parliamentary Election: What Are German Voters Sharing over Twitter?' (University of Oxford 2017) 1; Maria Martinez, 'Germany's Far-Right AfD Rises to Record 28%, INSA Poll Shows' *Reuters* (25 April 2026) <<https://www.reuters.com/world/germanys-far-right-afd-rises-record-28-insa-poll-shows-2026-04-25/>>.

²⁵ Chris Lunday, 'Putin's Bot Army Tries to Swing German Election' *POLITICO* (6 February 2025) <<https://www.politico.eu/article/germany-election-flood-social-media-x-russia-bots-kremlin-operation-false-news/>>; Federal Foreign Office, 'Germany Targeted by the Pro-Russian Disinformation Campaign "Doppelgänger"' (Federal Foreign Office 2024) Technical Report on an Analysis by the Federal Foreign Office 2,9 and 13 <<https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf>>.

²⁶ Aneta Zachová, 'TikTok Bots Push Anti-System Parties Ahead of Czech Elections' *EURACTIV* (2 October 2025) <<https://www.euractiv.com/news/tiktok-bots-push-anti-system-parties-ahead-of-czech-elections/>>.

²⁷ Paolo Cesarini, 'Propaganda and Disinformation: Lessons from 2024/25 Elections in Europe' *European Digital Media Observatory (EDMO)* (10 June 2025) <<https://edmo.eu/edmo-news/propaganda-and->

However, bots were also used on other platforms during the elections in Romania such as Meta platforms and X (formerly Twitter).²⁸ During the 2022 general election in Sweden, bots were identified as being responsible for around 22% of all election-related content.²⁹ But, political bots were also used on Twitter ahead of the 2018 general election in Sweden.³⁰

Moreover, Ferrara argues and proves that a black market may exist for reusable political disinformation bots employed across election campaigns.³¹ The study reveals that accounts used to support presidential candidate Donald Trump prior to the 2016 US presidential election were later reactivated.³² However, during the 2017 elections in France, after a period of inactivity, they were used to participate in the MacronLeaks disinformation campaign.³³

For politicians, the digital interactions enable remarkable opportunities—making it possible not just to pull a rabbit out of a hat but to pull a hat out of a rabbit! However, political elections, by their very nature, possess irreversible and unrepeatable characteristics. Once the elections are concluded, altering the results becomes nearly impossible, as such actions would undermine public trust in both the electoral process and in democracy itself. The same applies to any unfair

disinformation-lessons-from-2024-25-elections-in-europe/>; ‘What Happened on TikTok around the Annulled Romanian Presidential Election? An Investigation and Poll’ *Global Witness* (17 December 2024) <<https://globalwitness.org/en/campaigns/digital-threats/what-happened-on-tiktok-around-the-annulled-romanian-presidential-election-an-investigation-and-poll/>>.

²⁸ ‘Analysis of Social Media Presence of Romanian Presidential Candidates’ *European Digital Media Observatory (EDMO)* (29 April 2025) <<https://edmo.eu/edmo-news/analysis-of-social-media-presence-of-romanian-presidential-candidates/>>.

²⁹ Linus Wahlberg, ‘Twitter Bots as a Threat to Democracy: How Political Bots on Twitter Jeopardized Democratic Functions of the Online Public Sphere during the 2022 Swedish General Election’ (Master’s Thesis, Uppsala University 2022) 49.

³⁰ Johan Fernquist and others, ‘Twitter Bots and the Swedish Election’ in Mohammad A Tayebi, Uwe Glässer and David B Skillicorn (eds), *Open Source Intelligence and Cyber Crime* (Springer International Publishing 2020) 161 <https://doi.org/10.1007/978-3-030-41251-7_6> accessed 29 April 2026.

³¹ Emilio Ferrara, ‘Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election’ [2017] *First Monday* 3 <<https://doi.org/10.5210/fm.v22i8.8005>> accessed 29 April 2026.

³² More recently, the reusability of such bots has increasingly been conceptualized through the notion of “sleeper bots.” See more Jaiv Doshi and others, ‘Sleeper Social Bots: A New Generation of AI Disinformation Bots Are Already a Political Threat’ (arXiv, 2024) <<https://doi.org/10.48550/ARXIV.2408.12603>> accessed 2 March 2025.

³³ Ferrara, ‘Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election’ (n 31) 3.

treatment a candidate or political party might experience during the election process. Judicial proceedings do not halt the election process and often move at a slower pace.³⁴ As a result, allegations raised during elections may be proven after the fact, but these allegations and their impact on democratic processes cannot be undone. The electoral results can either resonate deeply within society or fade into obscurity, however, the point remains that the events leading up to the results are irreversible. This is because the allegations regarding the manipulation may not always be proven.

In the past two decades, digital platforms have expanded the information ecosystem,³⁵ a shift known as the transition from broadcast democracy to post-broadcast democracy.³⁶ The democratic process feels more like a scripted reality show, where the outcome can seem predetermined or staged.³⁷ Now, media can instantly gauge public reactions, something that was not possible before. People are more engaged, but they no longer simply watch the news. Instead, they follow celebrities and influencers, who openly share their political views and endorsements on social media platforms. This also constitutes a form of mediated information, as the content is filtered not only through the platform but also through the political leanings of these intermediaries, namely celebrities or influencers. So, elections may cover unwanted

³⁴ Particularly in authoritarian regimes, where judicial independence is questioned, the claim that these legal proceedings are deliberately postponed until after the electoral processes remains only an allegation.

³⁵ Robin Mansell and others, 'Information Ecosystems and Troubled Democracy A Global Synthesis of the State of Knowledge on News Media, AI and Data Governance' (The International Observatory on Information and Democracy, 2024) 12 and 79.

³⁶ Prior, in this book, highlights that "even the Internet, though diffusing very quickly in the 1990s, did not spread as fast as broadcast television." The book draws attention to the fact that changes in the media environment can influence politics, particularly when they change the composition of those likely to vote. It argues that "if less-educated citizens begin to learn about politics from broadcast news and vote more," their involvement may cause a moderating influence on electoral results. See Markus Prior, *Post-Broadcast Democracy: How Media Choice Increases Inequality in Political Involvement and Polarizes Elections* (Reprint, Cambridge University Press 2008) 18 and 59.

³⁷ Jonah Goldberg, 'Trump Turned Politics into Reality TV. Now Harris Is the Show to Watch' *Los Angeles Times* (13 August 2024) <<https://www.latimes.com/opinion/story/2024-08-13/donald-trump-campaign-kamala-harris-polling>>; Stefan L Brandt, 'Donald Trump, the Reality Show: Populism as Performance and Spectacle' (2020) 50 *Zeitschrift für Literaturwissenschaft und Linguistik* 303 <<https://doi.org/10.1007/s41244-020-00170-3>>.

components, such as foreign interventions³⁸, that threaten electoral integrity. Legal frameworks, including the Charter of Fundamental Rights of the European Union (CFR),³⁹ the Artificial Intelligence Act (AI Act),⁴⁰ the Regulation on the Transparency and Targeting of Political Advertising (TTPA),⁴¹ and other relevant regulations, could mitigate such concerns.

On the other hand, this shift calls into question the basic principles of democracy, particularly the importance of the secret ballot, and why it was originally introduced. The 2024 US presidential elections resembled a spectacle, with celebrities and influencers publicly endorsing candidates like Trump or Harris and influencing their followers.⁴² In this era, political powerbrokers find platforms that amplify their loud, multifaceted, disruptive, and far-reaching presence. Such dynamics often overlaps with the function of political bots on digital platforms.

It seems Elon Musk, as the owner of the social media platform X (formerly Twitter), filled this vacuum in 2024 for the presidential elections in the US. By spring 2023, Musk had dismissed approximately 80% of X's employees. This was widely regarded as a drastic reduction of the company's election integrity team.⁴³ Musk later openly supported a campaign candidate, Donald Trump. It appeared that X, while owned by Musk, potentially predicted the political

³⁸ 'New Allegations of Russian Interference in the European Parliament, in the Upcoming EU Elections and the Impact on the European Union (2024/2696(RSP))' (European Parliament 2024) <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0380_EN.html>.

³⁹ Even though the CFR predates the emergence of political bots and AI-driven electoral technologies, principles of democracy and rights such as freedom of expression (Article 11), the right to vote and stand as a candidate (Article 39) continue to provide the constitutional foundation for contemporary regulation of AI and political communication. Charter of Fundamental Rights of the European Union [2012/C 326/02] (Document C2012/326/02).

⁴⁰ Artificial Intelligence Act 2024 [2024/1689].

⁴¹ Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising 2024 [Document 32024R0900].

⁴² Maya Yang, 'Which Celebrities Have Endorsed Kamala Harris and Donald Trump? Here Are the Biggest Names' The Guardian (3 November 2024) <<https://www.theguardian.com/us-news/2024/nov/03/celebrity-endorsements-harris-trump>>.

⁴³ Paul M. Barrett and others, 'Digital Risks to the 2024 Elections: Safeguarding Democracy in an Era of Disinformation' (NYU Center for Business and Human Rights 2024) 6 <<https://bhr.stern.nyu.edu/publication/digital-risks-to-the-2024-elections-safeguarding-democracy-in-the-era-of-disinformation/>>.

preferences of platform users long before they reached the ballot box and he turned X into pro-Trump echo chamber.⁴⁴ Thus, the tendencies of voters can be predicted through non-transparent and non-traditional methods, beyond established voter behaviour prediction models.⁴⁵

Besides one of Trump's strongest supporters, Elon Musk, Jeff Bezos—the owner of The Washington Post—has also held one of the major broadcasting outlets in his hands. Yet Bezos does not occupy the same position as Musk, since the dynamics are quite different: traditional newspapers no longer hold the same level of influence over voters.⁴⁶ On the other hand, Daniel Ek, the Europe-based CEO of Spotify, was among the executives who met with Trump following his re-election in 2024.⁴⁷ It seems that the platform-owning powerbrokers are not exclusively US-based. However, these meetings also involved donations⁴⁸ to Trump's campaign—donations that, without doubt, were later expected to yield considerable returns.⁴⁹ Accordingly, novel tech powerbrokers, celebrities and influencers openly endorse candidates as a reflection of their own voices, something that is clearly protected under freedom of speech.

⁴⁴ David Ingram, 'How Elon Musk Turned X into a Pro-Trump Echo Chamber' BNC News (31 October 2024) <<https://www.nbcnews.com/tech/social-media/elon-musk-turned-x-trump-echo-chamber-rcna174321>>; Nick Robins-Early and Rachel Leingang, 'Elon Musk Is Trump's Biggest Cheerleader. How Could He Affect Election Results?' The Guardian (18 October 2024) <<https://www.theguardian.com/us-news/ng-interactive/2024/oct/18/elon-musk-trump-election-influence>>.

⁴⁵ Timothy Graham and Mark Andrejevic, 'A Computational Analysis of Potential Algorithmic Bias on Platform X during the 2024 US Election [Working Paper] (Unpublished)' (2024) <<https://eprints.qut.edu.au/253211/>>.

⁴⁶ Sophie James, 'Big Tech Emerges from US Election as New Powerbroker' centralnews <<https://centralnews.com.au/2024/11/14/big-tech-emerges-from-us-election-as-new-powerbroker/>>.

⁴⁷ Alayna Treene, Kristen Holmes and Jeremy Herb, 'How CEOs Are Trying to Be like Musk and Curry Favor with Trump' CNN (21 December 2024) <<https://edition.cnn.com/2024/12/21/politics/how-ceos-are-trying-to-be-like-musk-and-curry-favor-with-trump>>.

⁴⁸ Karen Weise and Maggie Haberman, 'Amazon Plans \$1 Million Donation to Trump's Inaugural Fund' (12 December 2024) <<https://www.nytimes.com/2024/12/12/technology/amazon-trump-inauguration.html>>.

⁴⁹ According to Bennett, donating is also becoming "quicker and more decentralised", particularly as modern technologies have fundamentally transformed the dynamics of political campaigning in the United States. See Colin J Bennett, 'Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America?' (2016) 6 International Data Privacy Law 261, 264; Also see Ari Levy and Lora Kolodny, 'Elon Musk Is \$70 Billion Richer since Trump Victory Due to Tesla Stock Surge' CNBC (11 November 2024) <<https://www.cnbc.com/2024/11/11/elon-musk-is-70-billion-richer-since-trump-victory-due-to-tesla-surge.html>>.

However, even when it comes to news consumption, digitally native younger generations tend to pay more attention to influencers and celebrities than to professional journalists.⁵⁰ Both these figures and the platforms they utilize have become key actors in the formation of political public opinion. This phenomenon has been known in the literature as ‘celebrity populism.’⁵¹ Nevertheless, these contemporary dynamics undermine the purpose of the secret ballot, which was introduced in the 1880s to prevent voter intimidation and protect the confidentiality of individual choices during public voting.⁵²

As a result, the questions surrounding democracy are not limited to these issues above. An essential aspect is how the legal framework can be defined and applied to protect democracy against the use of political bots in democratic processes. Thus this research aims to present a detailed socio-legal analysis of the potential influence of the EU’s AI Act on political bots from the perspective of freedom of expression and information (as articulated in Article 11 of the EU Charter).

⁵⁰ Catherine Kim, ‘How Gen Z Became the Most Gullible Generation’ (23 April 2025) <<https://www.politico.com/news/magazine/2025/04/23/gen-z-media-tiktok-misinformation-00287561>>; Tarja Laaninen, ‘Media Literacy Fostering a Key Civic Skill in a Digital Information Environment’ (European Parliament 2025) Briefing PE 772.886 <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772886/EPRS_BRI\(2025\)772886_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772886/EPRS_BRI(2025)772886_EN.pdf)>.

⁵¹ See more Silvija Vuković, ‘Celebrities Turning into Populists: The Celebrity Populism of Miroslav Škoro during the 2019 Croatian Presidential Campaign’ (2022) 13 *Medijske studije* 50 <<https://doi.org/10.20901/ms.13.25.3>>; Silvija Vuković, ‘Celebrity Populism and Leadership: Analyzing the Interplay of Celebrity Politics and Populism in Contemporary Political Communication’ (PhD Thesis, Charles University 2025) <<http://hdl.handle.net/20.500.11956/201166>>.

⁵² David S Tatel, ‘The Right to Vote’ (2015) 159 *Proceedings of the American Philosophical Society*.

The existing literature on political bots has predominantly emerged from the fields of media studies,⁵³ sociology,⁵⁴ and computer science,⁵⁵ and is particularly evolving towards the concept of computational politics.⁵⁶ In legal literature, political bots have mainly been addressed within the framework of election law through their technical characteristics, such as automation, as well as in relation to freedom of expression and information.⁵⁷ However, limited attention paid to the regulatory position of AI-powered political bots in the AI Act, particularly in relation to their potential impact on democratic processes. The AI Act introduces a risk-based framework for AI systems used in democratic processes in Annex III; it does not explicitly regulate political bots as a distinct category. This raises uncertainty about whether the existing legal framework, the AI Act, sufficiently and effectively addresses the risks posed by AI-driven political bots during democratic processes. As a result, this thesis addresses the potential gap by providing a multi-layered legal assessment of political bots in the AI Act and exploring whether a regulatory gap exists in the current framework.

⁵³ These are some examples from the literature, although the discussion is not limited to them. Monaco and Woolley (n 3); Samuel Woolley, *Manufacturing Consensus: Understanding Propaganda in the Era of Automation and Anonymity* (Yale University Press 2023); Samuel C Woolley and Philip N Howard (eds), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (Oxford University Press 2019).

⁵⁴ These are some examples from the literature, although the discussion is not limited to them. Philip N Howard, Samuel Woolley and Ryan Calo, 'Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration' (2018) 15 *Journal of Information Technology & Politics* 81 <<https://doi.org/10.1080/19331681.2018.1448735>>; Philip N Howard and Bence Kollanyi, 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum' <<https://doi.org/10.48550/ARXIV.1606.06356>> accessed 1 September 2023; Kollanyi, N. Howard and Woolley (n 21).

⁵⁵ These are some examples from the literature, although the discussion is not limited to them. Massimo Stella, Emilio Ferrara and Manlio De Domenico, 'Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems' (2018) 115 *Proceedings of the National Academy of Sciences* 12435 <<https://doi.org/10.1073/pnas.1803470115>>.

⁵⁶ Zeynep Tufekci, 'Engineering the Public: Big Data, Surveillance and Computational Politics' [2014] *First Monday* <<https://doi.org/10.5210/fm.v19i7.4901>> accessed 7 December 2022.

⁵⁷ Lamo and Calo (n 1); Philip N Howard, Samuel Woolley and Ryan Calo, 'Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration' (2018) 15 *Journal of Information Technology & Politics* 81 <<https://doi.org/10.1080/19331681.2018.1448735>>.

This thesis is guided by two research questions(RQs):

RQ1: How are political bots used as a tool for manipulation in political elections in Europe?

RQ2: How could the EU's AI Act prevent political bots from being used as a tool for manipulation without interfering with pluralism and freedom of expression and information?

1.1.2. Scope of the Research

These research questions prompt sub-questions to further clarify the concept of political bots in legal documents. The questions also explore the judicial perspective on the use of political bots in political election campaigns. As election campaigns are communication campaigns,⁵⁸ this research extends to the fields of communication studies, sociology, and media studies, thereby taking an interdisciplinary scope. However, it remains firmly grounded in a legal perspective.

In doing so, the research conceptualises democratic processes as the period beginning with the official announcement of the election or referendum and ending with the closing of the polls on election day. To explore these questions, the theoretical framework of the research is based on Habermas's arguments and the dynamics underlying the distinction between the private-public spheres.⁵⁹

In this research, the jurisdiction is clearly defined as the European Union (EU) and the decisions of the Court of Justice of the European Union (CJEU). This is because the research focuses on the AI Act, one of the recent regulations of the EU. The Act originally planned to apply many obligations for high-risk AI systems from 2 August 2026. However, EU AI Act Omnibus deal

⁵⁸ Martin Moore, '8. Protecting Democratic Legitimacy in a Digital Age' (2019) 90 *The Political Quarterly* 92 <<https://doi.org/10.1111/1467-923X.12572>>.

⁵⁹ Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (MIT Press 1989).

separates the timetable more clearly.⁶⁰ The compliance deadline for stand-alone high-risk AI systems was extended to 2 December 2027. The compliance deadline for AI embedded in regulated products was extended to 2 August 2028.⁶¹ This research engages with the AI Act because contemporary bots function as AI-driven models, meaning that they are programs within which AI is embedded. This establishes a clear link between AI and bots. Accordingly, it is important to examine how the AI Act regulates such systems and, more specifically, the legal framework it provides for political bots operating as AI-driven models.

At certain points, examples from other jurisdictions, particularly the United States⁶² and Turkey, are provided to support specific arguments.⁶³ These references primarily are intended

⁶⁰ European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) {SWD(2025) 836 final} 2025 [COM(2025) 836 final] (2025/0359 (COD)).

⁶¹ Pascale Davies, 'The New EU AI Act Is under Threat from Lobbyists, Experts and the Public Agree' (3 December 2023) <<https://www.euronews.com/next/2023/11/29/europes-ai-act-under-threat-by-lobbyists-experts-and-the-public-say>>.

⁶² The 2016 U.S. presidential election was not the first election in which bots were used. However, it was arguably the first case in which their use became a major global news story. For this reason, examples from the United States were also included in the study. In addition, the US has significantly influenced digital political communication practices beyond its own jurisdiction, including within Europe. As discussed in Web of Lies, developments in digital culture in Ireland, including political online narratives, have often followed trends that first emerged in the US. Consequently, the US context provides useful examples for understanding developments in political bots, computational propaganda, and digital political communication that may also be relevant within European democracies. Shiroma Silva, 'Trump's Twitter Debate Lead Was "Swelled by Bots"' *BBC News* (18 October 2016) <<https://www.bbc.com/news/technology-37684418>>; Aoife Gallagher, *Web of Lies: The Lure and Danger of Conspiracy Theories* (GILL BOOKS 2022).

⁶³ Examples from Turkey are also included in this thesis, in Section 2.4, "Governance of Political Bots Around Elections," and Section 2.2.2, "Are Political Bots the Digital Continuation of Traditional Media in Electoral Campaigns?" The reason for including examples from Turkey is that democratic system reflects signals of electoral autocracy, in which a democratic process gradually shifts toward authoritarian rule through elections. In other words, Turkey demonstrates patterns of democratic backsliding and electoral autocracy. Although similar patterns have also been observed in Hungary, the expected political changes following the 2026 elections may alter this situation. Therefore, despite not being an EU Member State, Turkey currently represents a distinct example within the broader European context. See details and the report on Hungary 'INTERIM REPORT on the Proposal for a Council Decision Determining, Pursuant to Article 7(1) of the Treaty on European Union, the Existence of a Clear Risk of a Serious Breach by Hungary of the Values on Which the Union Is Founded' (Committee on Civil Liberties, Justice and Home Affairs 2022) (C9-0000/2022 – 2018/0902R(NLE)) <https://web.archive.org/web/20230321060050/https://www.europarl.europa.eu/doceo/document/A-9-2022-0217_EN.html>; 'The Guardian View on Turkey's Election: An End to Erdoğan's Authoritarianism?' *The Guardian* (11 May 2023) <<https://www.theguardian.com/commentisfree/2023/may/11/the-guardian-view-on-turkeys-election-an-end-to-erdogans-authoritarianism>>; Zafer Yılmaz and Bryan S Turner, 'Turkey's Deepening Authoritarianism and the Fall of Electoral Democracy' (2019) 46 *British Journal of Middle Eastern Studies* 691, 692 <<https://doi.org/10.1080/13530194.2019.1642662>>.

to highlight potential risk that have not yet materialised within the EU.⁶⁴ They are also intended to outline expectations for ensuring more effective implementation of the AI Act without leaving legal gaps. Furthermore, the decision to limit the legal context of this research to the EU is based on the EU's leading role in regulating digital environment and its prioritisation of not only product and market interests, also broader public interests, including democracy and fundamental rights, within its regulatory framework.

Therefore, in this research, it is analysed through the dynamics underlying the theoretical framework, whether deliberative democracy is strengthened or undermined through political bots. This thesis then addresses how society perceives the use of political bots during political election processes, with insights gathered through interviews conducted with AI professionals. The research offers a law-in-context analysis within the framework outlined by the AI Act and EU law, and is therefore limited to the EU jurisdiction, while considering both the theoretical framework and the insights provided by AI professionals.

1.1.3. What is a Bot?

In order to understand the full story behind bots and political bots, as well as the questions and discussions, there is a need to first provide a conceptual overview of what bots are. Bots are computer algorithms.⁶⁵ They are used to generate text, communicate with humans or other robots, create audio responses, or provide visualised answers. Today, they are used for more

⁶⁴ As shown in previous studies, political bots had already been used in computational politics experiments in several non-EU countries, including the United States and Turkey. These studies refer to these earlier uses of political bots as “robotic lobbying.” See Michelle Forelle and others, ‘Political Bots and the Manipulation of Public Opinion in Venezuela’ (arXiv, 2015) 6 <<https://doi.org/10.48550/ARXIV.1507.07109>> accessed 16 June 2025; Philip N Howard and Bence Kollanyi, ‘Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum’ 5 <<https://doi.org/10.48550/ARXIV.1606.06356>> accessed 1 September 2023; More details can be found in this report also Samantha Bradshaw and Philip N. Howard, ‘The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation’ (Oxford Internet Institute 2019) Computational Propaganda Research Project.

⁶⁵ Keith Raymond Harris, ‘Liars and Trolls and Bots Online: The Problem of Fake Persons’ (2023) 36 *Philosophy & Technology* 35, 36; See the definition of algorithms: ‘Algorithmic Competition – Background Note’ (OECD Secretariat 2023) 7 <[https://one.oecd.org/document/DAF/COMP\(2023\)3/en/pdf](https://one.oecd.org/document/DAF/COMP(2023)3/en/pdf)>.

technical works such as coding, analysis data sets, medical diagnosis and treatment planning. There are various bots that can be utilized to respond, generate a video or sound, or generate any image considering some orders such as listener bot, spambots, wikiedits bots, sleeper bots, troll bots, honeypot.⁶⁶ This section focuses on what exactly bots are. Initially, all chatbots are bots, mostly conversational agents,⁶⁷ but not all bots are chatbots.⁶⁸

As a term, “chatbot” was coined by Mauldin⁶⁹ to describe systems capable of miming human interaction and passing the Turing Test.⁷⁰ The development of increasingly intelligent chatbots was led by the first chatbot ELIZA. Joseph Weizenbaum created the first functional chatbot at the Massachusetts Institute of Technology (MIT) in the US between 1964 and 1966.⁷¹ Eliza was the first computer program that could have a conversation with humans⁷² and inspired other chatbots such as Parry,⁷³ Alice,⁷⁴ and SmarterChild.⁷⁵

⁶⁶ Nathaniel Persily and Joshua A Tucker (eds), ‘Bots and Computational Propaganda: Automation for Communication and Control’ *Social Media and Democracy: The State of the Field, Prospects for Reform* (1st edn, Cambridge University Press 2020) <<https://doi.org/10.1017/9781108890960>> accessed 27 August 2023.

⁶⁷ Sheetal Kusal and others, ‘A Systematic Review of Applications of Natural Language Processing and Future Challenges with Special Emphasis in Text-Based Emotion Detection’ (2023) 56 *Artificial Intelligence Review* 15129 <<https://doi.org/10.1007/s10462-023-10509-0>>.

⁶⁸ Carlene R Lebeuf, ‘A Taxonomy of Software Bots: Towards a Deeper Understanding of Software Bot Characteristics’ (Master of Science, University of Victoria 2013) 24 <https://chisel.cs.uvic.ca/theses/Lebeuf_Carlene_MSc_2018.pdf>.

⁶⁹ Mauldin calls them a “Chatter Bot” and explained that they are “computer controlled players”. See Michael L Mauldin, ‘ChatterBots, TinyMuds, and the Turing Test: Entering the Loebner Prize Competition.’ (1994) 16.

⁷⁰ Turing test, is proposed by Alan Turing in 1950 to determine if a machine can ‘think’. See Alan Mathison Turing, ‘Computing Machinery and Intelligence’ (1950) 59 *Mind* 433, 433.

⁷¹ Simone Natale, ‘If Software Is Narrative: Joseph Weizenbaum, Artificial Intelligence and the Biographies of ELIZA’ (2019) 21 *New Media & Society* 712, 716 <<https://doi.org/10.1177/1461444818804980>>.

⁷² Lebeuf (n 68) 7.

⁷³ Vint Cerf, ‘PARRY Encounters the DOCTOR’ (1973) *Request for Comments: 439* NIC: 13771 <<https://www.rfc-editor.org/rfc/pdfrfc/rfc439.txt.pdf>>.

⁷⁴ Richard S Wallace, ‘The Anatomy of A.L.I.C.E.’ *Parsing the Turing Test* (2007) <https://doi.org/10.1007/978-1-4020-6710-5_13>.

⁷⁵ Nadine Lessio and Alexis Morris, ‘Toward Design Archetypes for Conversational Agent Personality’ 2020 *IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (IEEE 2020) 3222 <<https://doi.org/10.1109/SMC42975.2020.9283254>> accessed 31 August 2023.

Kenneth Mark Colby from Stanford's Psychiatry Department introduced another well-known chatbot PARRY in 1972.⁷⁶ When ELIZA and PARRY were used to rule-based orientation, bots were generating a reply with the most matching keywords, or the most similar wording pattern, from a database or hard coded rules. In the 1980s, ALICE used Artificial Intelligence Markup Language (AIML).⁷⁷ Julia was the first verbal chatbot in 1994.⁷⁸ Then, Sylvia became the first "virtual human" in 1997. In 2001, Smarterchild was the first successful consumer-oriented applications of natural language processing (NLP). This service was integrated with data sources that provided real-time information, thereby it provided news update, forecasts, stock quotes as well as interactive games and quizzes. What sets it apart from most existing chatbots is that it is sarcastic and snarky.⁷⁹ Therefore, until the Smarterchild in early 2000s, earlier chatbots could be considered text-based and they could categorize user-submitted words and phrases before matching the proper answer. Smarterchild, however, can be seen as the pioneer to contemporary chatbots.

Bots can be separated into two different categories based on their approaches to any input. These categories consist of rule-based chatbots and AI-driven models.⁸⁰ For the rule-based approach, a bot identifies specific patterns in the given input and applied these patterns to predefined rules. Rule-based chatbots follow a decision tree matrix to provide a specific action

⁷⁶ TL Grigorie (ed), Zemčík, M.T. (2019). *A Brief History of Chatbots. International Conference on Artificial Intelligence, Control and Automation Engineering (AICAE 2019): June 23-24, 2019, Wuhan, China* (DEStech Publications, Inc 2019) 144; OV Deryugina, 'Chatterbots' (2010) 37 Scientific and Technical Information Processing 143, 144 <<https://doi.org/10.3103/S0147688210020097>>.

⁷⁷ AIML is designed to create stimulus-response chat robots. This language is an XML (eXtensible Markup Language) which is a flexible, text-based markup language designed to store and transport data in a structured, both computer and human-readable format. See Wallace (n 74) 182.

⁷⁸ Mauldin (n 69) 19; Lebeuf (n 68) 7.

⁷⁹ One of the creators of the early instant-messaging bot SmarterChild, Robert Hoffer, says "If you offended SmarterChild you had hell to pay." Namely, Smarterchild felt as if the other party had a personality in a conversation with SmarterChild. See Shay Maunz, "'It Has To Have A Soul': How Chatbots Get Their Personalities" npr (10 March 2017) <<https://www.npr.org/sections/alltechconsidered/2017/03/10/519002884/it-has-to-have-a-soul-how-chatbots-get-their-personalities>>.

⁸⁰ For the legal assessment of AI-driven bots, see Chapter 3.

response, namely, evaluating and prioritising a list of options. Then, the bot selects an answer based on the closest matching command the predefined set of answers.⁸¹ This is why, the rule-based chatbots are unable to learn themselves as the rules for processing input are decided in advance. These bots are commonly employed for tasks such as booking a table at a restaurant, purchasing a movie ticket, or flight tickets or serving as a source of frequently asked questions (FAQs).

Over the years, developed technologies have introduced new capabilities of bots. They also generate more accurate responses using NLP, and demonstrate advanced capabilities on a much broader scope such as creative content generation, real-time language translation, or high-level problem solving to increase optimisation algorithms or productivity of computer systems. AI-driven bots analyse input comprehensively which can be a text, audio, or image. Then, they decide the context and the goal of the input, for this purpose AI-driven bots leverage Natural Language Understanding (NLU), NLP and Natural Language Generation (NLG). They apply machine learning algorithms trained on datasets to generate contextually appropriate responses. Additionally, AI driven bots can provide more accurate, relevant and human like responses.⁸² However, the data sets can include biases and lead to skewed outcomes. AI-driven bots, then, can amplify existing societal prejudices.⁸³ To address potential bias of AI-driven bots a collaborative effect between AI developers, users and affected communities is necessary.⁸⁴

The operation logic of these bots relied on predefined commands or prompts and limiting their NLP capabilities. This is why, they are categorised as chatbots but their operational capabilities

⁸¹ Saadat Izadi and Mohamad Forouzanfar, 'Error Correction and Adaptation in Conversational AI: A Review of Techniques and Applications in Chatbots' (2024) 5 AI 803, 807 <<https://doi.org/10.3390/ai5020041>>.

⁸² *ibid* 805.

⁸³ *ibid* 804.

⁸⁴ Emilio Ferrara, 'Should ChatGPT Be Biased? Challenges and Risks of Bias in Large Language Models' (2023) 28 15 <<https://doi.org/https://doi.org/10.5210/fm.v28i1.1.13346>> accessed 13 December 2024.

are far less than generative pre-trained transformers (GPT). Their popularity has significantly increased largely due to the release of OpenAI's ChatGPT, which was the first consumer facing model of ChatGPT, on 30 November 2022.

Before ChatGPT, bots were used for text or voice-based communication and assistance. Virtual assistants like Siri, Alexa and Google Assistant operated through voice commands. Text-based bots like Twitter bots and Facebook messenger bots interacted with users by providing information or updates such as weather forecasts in response to specific words on the platforms. They are also used to facilitate transcription, task automation, writing and analysing code, conducting research, creating and editing images, videos, sound, presentations. Microsoft's Cortana, Google Assistant, Microsoft's Tay and Cleverbot, and IBM's Watson are among the most advanced bots today and still being actively developed.

Bots have reached advanced level due to machine learning, data analytics and NLP,⁸⁵ NLU,⁸⁶ NLG,⁸⁷ and Generative Pre-Trained Transformer (GPT).⁸⁸ Large language models (LLMs) are deep learning models which are used for various purposes. They have been able to learn relationships between syntax and grammar across languages. For this reason, they process the form of language rather than its social meaning.⁸⁹ Thanks to pre-trained vast amounts of data,

⁸⁵ NLP covers all models based on textual data including unstructured language data. It makes human language accessible to computers. For this purpose, it converts unstructured language data to structured data format. Thus, it provides ability for computers to understand and generate human language.

⁸⁶ NLU is a subset of NLP and focuses on machine reading comprehension to determine the intended meaning of a sentence or text.

⁸⁷ NLG provides generated text as a result of given dataset.

⁸⁸ GPT is a type of large language model. It is based on a transformer deep learning architecture to generate human-like text. See Jayant Narayan and Benjamin Larsen, 'Generative AI: A Game-Changer That Society and Industry Need to Be Ready For' (World Economic Forum, 9 January 2023) <<https://www.weforum.org/stories/2023/01/davos23-generative-ai-a-game-changer-industries-and-society-code-developers/>>. Also see 'Report of the Work Undertaken by the ChatGPT Taskforce' (European Data Protection Board 2024).

⁸⁹ James Muldoon, Mark Graham and Callum Cant, *Feeding the Machine: The Hidden Human Labour Powering AI* (Canongate 2024) 164.

they can respond to human language. Also, they are based on neural network architecture, specifically transformer models, as seen in GPT or commonly ChatGPT. The amount of data is collected by using web scraping. Web scraping is a way to train these models by having publicly available resources. They can use automated collection and extraction of certain information from different publicly available sources. The resources can include personal data.⁹⁰

Consequently, in the 20th century, meaningful communication between humans and machines was established. Generative AI has caused a massive transformation in AI-driven bots since 2022. Prominent examples of generative AI include OpenAI's ChatGPT, Copilot, Gemini and Bard. Generative AI refers to AI software systems that have been trained on amounts of data to communicate in natural language. These systems are able to respond to relatively complex questions, to formulated queries and follow instructions or prompts thanks to training on vast amounts of datasets. Generative AI works by learning patterns and characteristics from large collections of data. Their whole working system relies on a statistical understanding of language.⁹¹ The main purpose is to define, with the greatest possible certainty, the next word, without knowledge of its own. This is why we can say they have a “probabilistic nature of system.”⁹²

Therefore, the working principle of generative AI is not based on the “knowledge”, but rather on using the statistical relationship derived from often combined words or concepts, namely patterns, to reach a conclusion regarding the ordered prompt by users. This is drawing

⁹⁰ The legal assessment is conducted in Chapter 3.

⁹¹ ‘Information Note on “Use of Generative Artificial Intelligence (AI) by Judicial Professionals in a Work-Related Context”’ (European Commission for the Efficiency of Justice(CEPEJ) Working group on Cyberjustice and Artificial Intelligence (CEPEJ-GT-CYBERJUST) 2024) CEPEJ-GT-CYBERJUST(2023)5final 2.

⁹² ‘Report of the Work Undertaken by the ChatGPT Taskforce’ (n 88) 8.

inferences from possible outputs. For instance, while an AI model may not know Dublin as the capital of Ireland, it makes an inference based on the association between the words "Ireland" and "Dublin" because these two words often appear together in the datasets. As a result, generative AI models encompass LLMs.

1.1.4. What are Political Bots?

Political bots, in turn, are a type of social bot. According to Woolley, social bots are software programs designed to mimic human social media users on social media platforms.⁹³ These platforms could be various, for instance, Facebook, Twitter, and Reddit. Technological developments led to expanding Woolley's definition describing social bots as programs "designed for one- or many-sided communication and the imitation of human online behaviour."⁹⁴ This capability results in their assimilation into communities of benign users.⁹⁵ The range of platforms on which social bots are used has also diversified, now including Instagram,⁹⁶ TikTok,⁹⁷ YouTube,⁹⁸ and LinkedIn.⁹⁹

⁹³ Samuel C Woolley, 'Automating Power: Social Bot Interference in Global Politics' [2016] First Monday <<https://doi.org/10.5210/fm.v21i4.6161>> accessed 25 February 2025.

⁹⁴ Dennis Assenmacher and others, 'Demystifying Social Bots: On the Intelligence of Automated Social Media Actors' (2020) 6 Social Media + Society 205630512093926, 1 <<https://doi.org/10.1177/2056305120939264>>.

⁹⁵ Seung Ho Na, Sumin Cho and Seungwon Shin, 'Evolving Bots: The New Generation of Comment Bots and Their Underlying Scam Campaigns in YouTube' *Proceedings of the 2023 ACM on Internet Measurement Conference* (ACM 2023) 297 <<https://doi.org/10.1145/3618257.3624822>> accessed 24 April 2026.

⁹⁶ Koosha Zarei, Reza Farahbakhsh and Noel Crespi, 'How Impersonators Exploit Instagram to Generate Fake Engagement?' *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)* (IEEE 2020) 4 <<https://doi.org/10.1109/ICC40277.2020.9149431>> accessed 24 April 2026.

⁹⁷ Yuliia Dukach, 'How TikTok Is Turning into an AI Dump. A Study of a Russian-Language Pirate TikTok Farm' (*Tekcmu.org.ua*, 10 May 2024) <<https://texty.org.ua/articles/112437/how-tiktok-turning-ai-dump-study-russian-language-pirate-tiktok-farm/>>.

⁹⁸ Na, Cho and Shin (n 95) 297.

⁹⁹ Stacy Hein, 'A Qualitative Study on How Micro-Influencers Detect Bots on LinkedIn' (PhD Thesis, Department of Doctoral Studies, Colorado Technical University 2023) 49 <<https://may.idm.oclc.org/login?url=https://www.proquest.com/dissertations-theses/qualitative-study-on-how-micro-influencers-detect/docview/2864746549/se-2?accountid=12309>>.

Social bots can shape social media agendas by employing hashtags (i.e., the use of the “#” symbol in content) to promote certain topics into trending status.¹⁰⁰ This is facilitated by their scale, coordination, and speed.¹⁰¹ Consequently, they can direct human users’ attention to particular issues. As real users seek to understand what trend topic is and why it is trending, they may be exposed to bot-generated and disseminated content associated with these hashtags. This is because, when users search for or click on a hashtag (the “#” symbol in content), they are more likely to find bot-generated content on social media platforms.¹⁰² Such visibility is enabled by bots’ capability to systematically amplify their own content and endorse one another bots, thereby pushing their posts to the forefront. This also indicates their ability to learn how social media algorithms function and to use them effectively. In this way, social bots can achieve their objective of spreading information or misinformation.¹⁰³

Moreover, by liking or endorsing content, social bots can influence real users and create the impression of support or opposition for a particular individual or idea.¹⁰⁴ Accounts with many followers are often perceived as more popular and more trustworthy by real users.¹⁰⁵ However,

¹⁰⁰ Nathaniel Persily, ‘Can Democracy Survive the Internet?’ (2017) 28 *Journal of Democracy* 63, 70 <<https://doi.org/10.1353/jod.2017.0025>>.

¹⁰¹ For instance, a study on bot activity related to vaccination found that bots are significantly more likely than average Twitter users to tweet about vaccination. This research shows their speed and coordination. See David A Broniatowski and others, ‘Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate’ (2018) 108 *American Journal of Public Health* 1378, 1380 <<https://doi.org/10.2105/AJPH.2018.304567>>.

¹⁰² Emilio Ferrara, ‘How Twitter Bots Affected the US Presidential Campaign’ *The Conversation* (8 November 2016) <<https://theconversation.com/how-twitter-bots-affected-the-us-presidential-campaign-68406>>.

¹⁰³ Persily (n 100) 70.

¹⁰⁴ This dynamic is highlighted in Citation 5 of this thesis on the case of Sinan Oğan. See Loni Hagen and others, ‘Rise of the Machines? Examining the Influence of Social Bots on a Political Discussion Network’ (2022) 40 *Social Science Computer Review* 264, 266 <<https://doi.org/10.1177/0894439320908190>>.

¹⁰⁵ In the literature, this phenomenon is conceptualized as “social proof.” Although social proof is generally understood as a psychological and social phenomenon, it is also widely used in marketing to build credibility. Rather than engaging in in-depth assessment, real users may rely on follower numbers for credibility and, consequently, may be more inclined to trust the content shared by such accounts. See more *ibid*; Seung-A Annie Jin and Joe Phua, ‘Following Celebrities’ Tweets About Brands: The Impact of Twitter-Based Electronic Word-of-Mouth on Consumers’ Source Credibility Perception, Buying Intention, and Social Identification With Celebrities’ (2014) 43 *Journal of Advertising* 181, 193 <<https://doi.org/10.1080/00913367.2013.827606>>.

in some cases, social bots have been observed to circulate or promote links to fake news sites, unreliable stories, and unverified rumours.¹⁰⁶

Woolley approaches political bots from the perspective of social bots and refers to a specific category of social bots, namely “politicised social bots.”¹⁰⁷ This approach provides a conceptual framework for understanding political bots in relation to social bots. Accordingly, politicised social bots are employed to “massively boost politicians’ follower levels on social media sites in attempts to generate false impressions of popularity.”¹⁰⁸ What differentiates political bots from social bots is that they are equipped with features to generate automated interactions¹⁰⁹ with other users about politics. As a result, the perspective of this thesis focuses on the potential disruption to democracy resulting from the manipulative use of political bots. This is because they are often designed to look and act like real people in order to manipulate public opinion.¹¹⁰ However, what is the most significant is that political bots are used for political purposes. These political purposes are diverse and can manifest in various forms.

For instance, political bots have often been implicated in the spread of misinformation.¹¹¹ Moreover, they can facilitate and amplify the spreading of misinformation, disseminate fake

¹⁰⁶ POLITICO Staff, ‘Incoming National Security Adviser’s Son Spreads Fake News about D.C. Pizza Shop’ *POLITICO* (12 April 2016) <<https://www.politico.com/story/2016/12/incoming-national-security-advisers-son-spreads-fake-news-about-dc-pizza-shop-232181>>; Persily (n 100) 68.

¹⁰⁷ Woolley (n 93).

¹⁰⁸ According to Keller and Klinger, Social bots can make actors appear more popular and socially acceptable than they really are. They can encourage other users to follow or “like” them. See more Keller and Klinger (n 14) 3; Woolley (n 93).

¹⁰⁹ Howard, Woolley and Calo, ‘Algorithms, Bots, and Political Communication in the US 2016 Election’ (n 57).

¹¹⁰ Nathaniel Persily and Joshua A Tucker (eds), *Social Media and Democracy: The State of the Field, Prospects for Reform* (1st edn, Cambridge University Press 2020) 93 <<https://doi.org/10.1017/9781108890960>> accessed 26 April 2023; Ratkiewicz and others (n 12); Piers Robinson, Philip Seib and Romy Frohlich (eds), ‘Social Media, Revolution, and the Rise of the Political Bot’ *Routledge Handbook of Media, Conflict and Security* (0 edn, Routledge 2016) <<https://doi.org/10.4324/9781315850979>> accessed 31 August 2023.

¹¹¹ Harris (n 65).

news,¹¹² trolling and propaganda.¹¹³ There can be more than generating artificial agenda in society or spreading disinformation, like ‘zombie electioneering’.¹¹⁴ Additionally, they can be used to mitigate the burden of troublesome online conversations such as managing repetitive or conflictual conversations during political campaigns.¹¹⁵

It is known that the first team organised for strategic and systematic online manipulation, which would later evolve into processes involving political bots, was established in China. This information was leaked by a government report from 2006.¹¹⁶ The manipulation of the decision-making process during elections started with internet trolls. According to Bolsover (2017), China’s “50-Cent Party” or *Wumao* was supposed to be an army of individuals who were paid 50 cents per post to support the state campaigns online.¹¹⁷ Indeed, as Robgin states in 2015, they are either online commentators or public servants and received their payment per-piece of comment.¹¹⁸

Subsequently, other countries will recognise how disruptive online manipulation is and will seek ways to develop and implement a faster, cheaper, and more effective strategy through an automated system, rather than relying on human involvement. Russia is one example that

¹¹² Jorge Rodríguez-Ruiz and others, ‘A One-Class Classification Approach for Bot Detection on Twitter’ (2020) 91 Computers & Security 101715, 11 <<https://doi.org/10.1016/j.cose.2020.101715>>.

¹¹³ Persily and Tucker (n 66).

¹¹⁴ If zombie electioneering is activated, bot accounts share their opinions, and links to online resources and campaign staff do not involve interacting with opinion voters, or leaders, or political opponents. See Howard, Woolley and Calo, ‘Algorithms, Bots, and Political Communication in the US 2016 Election’ (n 57) 87.

¹¹⁵ Persily and Tucker (n 66).

¹¹⁶ The original source is in Chinese, which is why the research that cited the original source is referenced here. See Xiaofeng Yang, Qian Yang and Christo Wilson, ‘Penny for Your Thoughts: Searching for the 50 Cent Party on Sina Weibo’ (2021) 9 Proceedings of the International AAAI Conference on Web and Social Media 694, 695 <<https://doi.org/10.1609/icwsm.v9i1.14649>>.

¹¹⁷ Gillian Bolsover, ‘Computational Propaganda in China: An Alternative Model of a Widespread Practice’ (2017) Working Paper No. 2017.4 7.

¹¹⁸ Han Rongbin, ‘Manufacturing Consent in Cyberspace: China’s “Fifty-Cent Army”’ (2015) 44 Journal of Current Chinese Affairs 105, 113 <<https://doi.org/10.1177/186810261504400205>>.

shows online manipulation via bots also used by governments, militaries, corporations and other well-resourced entities to launch offensives online.¹¹⁹

The Russian government adopted bots and trolls as key propaganda tools, and developed crucial expertise using them during the crisis.¹²⁰ Similarly, the first known large-scale deployment of pro-government bots and trolls in Russia engaged in the typical “50-cent-ers” activities.¹²¹ The activities evolved progressively over the years, and by the early 2000s, Russia had a well-established and innovative industry in spam and search optimization,¹²² among other things. As a result, this advantage became a key commercial technology initiative for the Russian government.¹²³

Thereafter, political bots were used in the Scottish Referendum in 2014, the Brexit referendum¹²⁴ in 2016, the US Presidential elections in 2016,¹²⁵ and during Catalan referendum in 2017.¹²⁶ This trend persisted in subsequent elections, including the 2017 presidential

¹¹⁹ Persily and Tucker (n 66).

¹²⁰ Sergey Sanovich, ‘Computational Propaganda in Russia: The Origins of Digital Misinformation’ Working Paper Working Paper No. 2017.3 6.

¹²¹ *ibid* 9.

¹²² Denis Stukal and others, ‘For Whom the Bot Tolls: A Neural Networks Approach to Measuring Political Orientation of Twitter Bots in Russia’ (2019) 9 SAGE Open 215824401982771, 13 <<https://doi.org/10.1177/2158244019827715>>; Sanovich (n 120) 9.

¹²³ Sanovich (n 120) 9.

¹²⁴ Matteo Bruno, Renaud Lambiotte and Fabio Saracco, ‘Brexit and Bots: Characterizing the Behaviour of Automated Accounts on Twitter during the UK Election’ (2022) 11 EPJ Data Science 17, 17 and 19 <<https://doi.org/10.1140/epjds/s13688-022-00330-0>>; Marco Bastos, Dan Mercea and Andrea Baronchelli, ‘The Geographic Embedding of Online Echo Chambers: Evidence from the Brexit Campaign’ (2018) 13 PLOS ONE e0206841 <<https://doi.org/10.1371/journal.pone.0206841>>.

¹²⁵ Kollanyi, Howard and Woolley (n 17).

¹²⁶ Massimo Stella, Emilio Ferrara and Manlio De Domenico, ‘Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems’ (2018) 115 Proceedings of the National Academy of Sciences 12435 <<https://doi.org/10.1073/pnas.1803470115>>.

election in France,¹²⁷ the 2017 parliamentary election in Germany,¹²⁸ the 2022 general election in Sweden,¹²⁹ and the 2024–2025 presidential elections in Croatia.¹³⁰

Howard highlights how political bots played “a small but strategic role” in shaping conversations on Twitter.¹³¹ In political campaigns, hashtags,¹³² echo chambers,¹³³ modifying public perception,¹³⁴ and polarising societies¹³⁵ were predominant. Among these, the forming and at times reshaping of public perception emerge as a particularly effective strategy. This is because the strategy can rescue an election campaign or a candidate during a turbulent political campaign period, or lead to its loss. Namely, the strategy may influence electoral dynamics, for example, by determining whether certain candidates withdraw from or remain in electoral

¹²⁷ Ferrara, ‘Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election’ (n 31).

¹²⁸ Lisa-Maria N. Neudert, ‘Computational Propaganda in Germany: A Cautionary Tale’ (2017) Computational Propaganda Research Project Working Paper No. 2017.7 11.

¹²⁹ Linus Wahlberg (n 29).

¹³⁰ ‘Inauthentic & Maligned Influence Activity - Croatian Presidential Runoff’ (Center for Information Resilience 2024) 4 <https://www.info-res.org/app/uploads/2025/01/Inauthentic_Behavior_-_Croatian_Presidential_Runoff_v2.pdf>.

¹³¹ Howard asserts that bots played a crucial role in the UK Brexit referendum. However, numerous studies provide evidence of their influence in other electoral contexts. See Samuel C Woolley and Philip N Howard, ‘Computational Propaganda Worldwide: Executive Summary’ Working Paper 2017.11 7; Bello and Heckel (n 11); Bessi and Ferrara (n 17); Başak Bozkurt, Diara J. Townes and Linda Li, ‘Election Interference: How Tech, Race, and Disinformation Can Influence the U.S Election’ (*Oxford Internet Institute*, October 2024) <<https://www.oii.ox.ac.uk/news-events/election-interference-how-tech-race-and-disinformation-can-influence-the-us-elections/>>; Stukal and others, ‘For Whom the Bot Tolls’ (n 122); Denis Stukal and others, ‘Why Botter: How Pro-Government Bots Fight Opposition in Russia’ (2022) 116 *American Political Science Review* 843 <<https://doi.org/10.1017/S0003055421001507>>.

¹³² During Brexit, the hashtags associated with the argument for leaving the EU were dominant. See Howard and Kollanyi (n 54) 5.

¹³³ See details Bastos, Mercea and Baronchelli (n 124); Michael Bossetta, Anamaria Dutceac Segesten and Hans-Jörg Trenz, ‘The Brexit Battle on Facebook: Assessing Echo Chambers and Polarisation’ (19 June 2018) <<https://blogs.lse.ac.uk/brexit/2018/06/19/the-brexit-battle-on-facebook-assessing-echo-chambers-and-polarisation/>>; Ros Taylor, ‘The Brexit Battle on Facebook: Assessing Echo Chambers and Polarisation’ (*LSE BREXIT Blog*, 19 June 2018) <<https://blogs.lse.ac.uk/brexit/2018/06/19/the-brexit-battle-on-facebook-assessing-echo-chambers-and-polarisation/>>.

¹³⁴ See details Forelle and others (n 64).

¹³⁵ Philip N Howard and others, ‘Social Media, News and Political Information during the US Election: Was Polarizing Content Concentrated in Swing States?’ <<https://doi.org/10.48550/ARXIV.1802.03573>> accessed 6 January 2023; Prior (n 36); Anja Prummer, ‘Micro-Targeting and Polarization’ (2020) 188 *Journal of Public Economics* 104210 <<https://doi.org/10.1016/j.jpubeco.2020.104210>>; Joshua Tucker and others, ‘Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature’ [2018] SSRN Electronic Journal <<https://doi.org/10.2139/ssrn.3144139>> accessed 15 September 2023.

race.¹³⁶ At this point, public perception appears to be closely related to use of political bots for manipulative purposes during democratic processes.¹³⁷ As Woolley highlights “bots do have influence on perceptions of a candidate’s political cachet.”¹³⁸ Thus, political bots may steer public perception during democratic processes. In this research, the insights from the interviewees (in Chapter 4) repeatedly emphasised their concerns about artificial amplification of political messages and political narratives the creation of misleading indicators of public support, such as manipulated or misrepresented surveys and public opinion polls, and the difficulties of identifying the influence of bots on public discourse. Indeed, it remains difficult to fully understand how online political discourse shapes public opinion and the extent to which bots influence public sentiment.¹³⁹

However, it is widely recognised that powerful political actors are using politicized ‘social bots’ for political electoral campaigns on a global scale and it is not limited to just a few countries or isolated political situations.¹⁴⁰ This is a novel mechanism of political communication, which can be defined as the algorithmic communication.¹⁴¹ This is because “campaigns follow voters”;¹⁴² that is, they follow the migration of voters to online platforms.

¹³⁶ Discrediting candidates and managing or reshaping public perception in democratic processes is not a new phenomenon. However, it is now conducted through online platforms. Even the presence of such activities on online platforms means that citizens become targets of public perception management, if not directly, then indirectly. Because television, still a widely used communication medium, transmits also online news and developments. So, when these strategies originate in digital environments, citizens may still be exposed to them indirectly via traditional media. As a result, traditional media remain widely used channels for conveying electoral and political updates from new media. Thus, even individuals who are not users of digital platforms can still be informed, as traditional media continue to compete with new media by incorporating and broadcasting online content.

¹³⁷ The relationship between the public perception concept and the thesis research question is significant. Because the strategy of managing public perception in democratic processes is facilitated or strengthened by the use of political bots.

¹³⁸ Woolley (n 53) 76.

¹³⁹ Woolley and Howard (n 131) 7.

¹⁴⁰ The relevant cases show that political bots are used for referendums, presidential election, general elections. Also see Howard, Woolley and Calo, ‘Algorithms, Bots, and Political Communication in the US 2016 Election’ (n 57).

¹⁴¹ Thomas Christiano, ‘Algorithms, Manipulation, and Democracy’ (2022) 52 *Canadian Journal of Philosophy* 109 <<https://doi.org/10.1017/can.2021.29>>.

¹⁴² Moore also emphasises “In many democracies, more than three-quarters of the adult population is online.” Moore (n 58) 92.

The strategic use of political bots as a part of election campaigns on digital platforms poses a significant threat to democratic processes, as citizens face manipulation through tactics such as misinformation, disinformation, and deepfakes.¹⁴³ Moreover, this communication strategy, algorithmic communication, may pose a threat to political equality, as most citizens engage in democratic decision-making with limited time, money, and energy, particularly under conditions of hypernudging.¹⁴⁴ Yet, public discussion is a prerequisite for making informed choices as a democratic citizen.¹⁴⁵ However, this thesis does not rely on the assumption that participation in online political debate is equivalent to voting status. Not all participants in public debate, whether online or offline, are voters or citizens. Rather, the concern is that political bots may shape public discourse and the wider information environment, although generally within digital environments surrounding democratic processes.¹⁴⁶

Today, public debate is ubiquitous across digital platforms.¹⁴⁷ It is also guided, and at times manipulated, by various impersonating profiles even if this is not a new phenomenon.¹⁴⁸

¹⁴³ Anna Caprile, 'Foreign Interference in EU Democratic Processes: Second Report' (European Parliament 2023) Plenary

<[https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747908/EPRS_ATA\(2023\)747908_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747908/EPRS_ATA(2023)747908_EN.pdf)>; Ethan Bueno de Mesquita, Brandice Canes-Wrone and Andrew B. Hall, 'Preparing for Generative AI in the 2024 Election' (Stanford Graduate School of Business and the University of Chicago Harris School of Public Policy November 2023) <https://harris.uchicago.edu/files/ai_and_elections_best_practices_no_embargo.pdf>.

¹⁴⁴ Christiano (n 141) 109.

¹⁴⁵ Jürgen Habermas, 'Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere' (2022) 39 *Theory, Culture & Society* 145, 160 <<https://doi.org/10.1177/02632764221112341>>; Jussi Salmi, 'A Democratic Way of Controlling Artificial General Intelligence' (2023) 38 *AI & SOCIETY* 1785, 1785 <<https://doi.org/10.1007/s00146-022-01426-x>>.

¹⁴⁶ A very recent research proves that LLMs silently shape the text on the platforms where people interact and engage. The research focuses on the biased content, and if such biased content is shared on large-scale online platforms, it has the potential to slowly

shift collective opinion and sway political views or influence voting behaviour. See more Stratis Tsirtsis and others, 'AI-Mediated Communication Can Steer Collective Opinion' (arXiv, 2026) 12

<<https://doi.org/10.48550/ARXIV.2605.16245>> accessed 19 July 2026.

¹⁴⁷ Ib T Gulbrandsen and Sine N Just, 'What Do We Know about Digital Public Debate? Technological Affordances and Democratic Dilemmas' (2025) 46 *Nordicom Review* 148, 148 <<https://doi.org/10.2478/nor-2025-0014>>.

¹⁴⁸ However, Sudmann highlights that "the influence of AI systems is often not rooted in technology but attributed to AI through social choices." Thus, this tendency toward manipulation does not exclude the role of AI itself, it also reflects social choices, such as society's inclination to engage in online discussion as a primary

Moreover, digital platforms facilitate the “formation of fragmented spheres of engagement”¹⁴⁹ by generating echo chambers or filter bubbles. As public debate becomes increasingly widespread on these platforms, the content circulated to users tends to consist of polarised or partisan modes of expression.¹⁵⁰ This, in turn, contributes to the division of publics rather than fostering collective deliberation. Here, political bots for manipulative purposes remain still significant tools and pose a threat to participatory and deliberative democracy.¹⁵¹

In conclusion, this research on the legal framework of political bots is crucial for one primary reason, and several secondary reasons. The main reason is that every time EU democracies are challenged by the threats posed by emerging technologies, their democratic resilience is effectively being tested and gradually eroded. Political bots are just one link in this chain of erosion, but contrary to popular belief,¹⁵² they are neither insignificant nor uncoordinated. On the contrary, they are small yet strategic agents that are embedded within, and in many ways constitute, the very core of the key challenges that must be addressed for the establishment of a strong democracy, including disinformation, fake news, and related threats.

mode of interaction. Andreas Sudmann (ed), *The Democratization of Artificial Intelligence: Net Politics in the Era of Learning Algorithms*, vol 1 (1st edn, transcript Verlag 2019) 27

<<https://doi.org/10.14361/9783839447192>> accessed 20 October 2025.

¹⁴⁹ Gulbrandsen and Just (n 147) 150.

¹⁵⁰ *ibid.*

¹⁵¹ ‘No Ifs, Many Bots? Partisan Bot-like Accounts Continue to Amplify Divisive Content on X, Generating over 4 Billion Views since the UK General Election Was Called’ (Global Witness 2024) <<https://www.globalwitness.org/en/campaigns/digital-threats/no-ifs-many-bots-partisan-bot-accounts-continue-amplify-divisive-content-x-generating-over-4-billion-views-uk-general-election-was-called/>>; Paul M Barrett, Justin Hendrix and Cecely Richard- Carvajal, ‘Digital Risks to the 2024 Elections: Safeguarding Democracy in an Era of Disinformation’ (NYU Center for Business and Human Rights 2024).

¹⁵² In the initial drafts of the AI Act, bots were classified as harmless AI systems, at least until the ChatGPT revolution shifted the future of tech from the LLMs' perspective. Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021 (COM/2021/206 Final).

For the several secondary considerations, first, political bots are difficult to detect,¹⁵³ and it is also challenging to determine the extent of their influence on society.¹⁵⁴ Research shows that bots change their stance far less frequently than humans.¹⁵⁵ Moreover, humans tend to express stronger positive sentiments than bots, with a similar trend observed in the expression of negative sentiments.¹⁵⁶ Thus, classifying Twitter users as either bots or humans remains a significant challenge. Although their threat to democracy is widely accepted, the measurement of the threat and potential harms in society remains almost impossible.

Second, there is a growing concern that society's trust in, and commitment to, the concept of media, government and democracy may erode.¹⁵⁷ As a response to targeting democracy and collective manipulations operated by political bots, it becomes impossible to determine the compensation for this harm. Namely, when democracy is undermined, the damage is already done, and there is generally no real way back until the next election cycle. Thus, there is a clear need for greater attention to protection of fundamental rights, such as right to assembly, freedom of expression and information, right to assembly that are closely tied to democratic

¹⁵³ Emilio Ferrara, 'Social Bot Detection in the Age of ChatGPT: Challenges and Opportunities' [2023] First Monday 19 <<https://doi.org/10.5210/fm.v28i6.13185>> accessed 26 November 2024; Howard, Woolley and Calo, 'Algorithms, Bots, and Political Communication in the US 2016 Election' (n 57) 84; Sanovich (n 120) 4; Başak Bozkurt, Diara J. Townes and Linda Li (n 131).

¹⁵⁴ Johan Fernquist, Lisa Kaati and Ralph Schroeder, 'Political Bots and the Swedish General Election' 2018 *IEEE International Conference on Intelligence and Security Informatics (ISI)* (IEEE 2018) 125 <<https://doi.org/10.1109/ISI.2018.8587347>> accessed 20 April 2023.

¹⁵⁵ John P Dickerson, Vadim Kagan and VS Subrahmanian, 'Using Sentiment to Detect Bots on Twitter: Are Humans More Opinionated than Bots?' 2014 *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)* (IEEE 2014) <<https://doi.org/10.1109/ASONAM.2014.6921650>> accessed 19 October 2025.

¹⁵⁶ *ibid.*

¹⁵⁷ In the Code of Conduct for the 2024 European Parliament Elections, it was emphasised that signatories commit to preventing the deliberate deception of the public, notably through the misuse of AI, as well as to strengthening the integrity of the electoral process and supporting public trust in democracy. Muldoon et al. argue in their book that "Generative AI could spread false information and supercharge propaganda during any future election campaigns, leading to a further erosion of trust in the media and government." To this erosion, one might also add democracy itself, as it is directly undermined by such dynamics. See more James Muldoon, Mark Graham and Callum Cant, *Feeding the Machine: The Hidden Human Labour Powering AI* (Canongate 2024) 41; 'Code of Conduct for the 2024 European Parliament Elections' (International Institute for Democracy and Electoral Assistance (International IDEA) and the European Commission 2024) 1 <https://commission.europa.eu/document/bebd9b72-fbb9-42f3-bcea-dbae7e0650f_en>.

processes. This research puts forward a core argument: without protecting democracy and electoral processes, it is unrealistic to expect broader human rights and fundamental rights to be upheld fairly and effectively in any society.¹⁵⁸

Third, there is a possibility that intense political campaigning within democratic processes may dull public awareness of the pursuit of rights. This is because democratic processes, which take place once every four or five years, are essentially short-term forms of public participation that briefly intensify public attention. In fact, it is a consensus-building process that requires society's attention for a limited period. However, election campaigns have increasingly been conducted through strategies that first foster polarisation within society and then focus heavily on undecided voters. Moreover, one of the common internet metaphors suggests that one human year equals seven internet years.¹⁵⁹ This accelerated timeline makes political bots an even greater threat to democracy: when undecided voters are targeted and exposed to them, such strategies may still influence electoral outcomes despite the shorter time frame. In conclusion, the intensity of rights violations in the non-transparent digital public sphere during democratic processes may give rise to a form of unconscious avoidance of rights-claiming. This is because such violations not only carry profiling characteristics that affect each voter

¹⁵⁸ The main claim here is that democracy serves as the ultimate guarantee for all other rights and freedoms. Only within a political and legal atmosphere in which democracy is protected can other fundamental rights truly be safeguarded. Behind this claim lies the belief that in a country where democracy and democratic processes are not protected, meritocracy will erode, public trust in the legal system and state institutions will decline, and as a result, corruption will drive the country into deeper crises. This claim reflects an approach to human rights theory that the researcher intended to argue in her master's thesis but could not fully address due to the restrictions of academic freedom at the time, and which is planned to be further developed in future work. See the thesis Gizem YARDIMCI, 'Avrupa İnsan Hakları Mahkemesi kararlarıyla serbest seçim hakkı (in English "The right to free elections in the decisions of the European Court of Human Rights")' (Published master's thesis, Ankara University 2020).

¹⁵⁹ Bella Dicks and others, *Qualitative Research and Hypermedia* (SAGE Publications, Ltd 2005) 29 <<https://methods.sagepub.com/book/qualitative-research-and-hypermedia>> accessed 1 September 2025; Karl Taro Greenfeld, 'The Network Effect' (10 April 2000) <<https://time.com/archive/6740836/the-network-effect/>>; Josh Bland, 'Expert Interview: What the Internet and Dog Years Have in Common' (13 January 2016) <<https://solutions.technologyadvice.com/blog/expert-interview-what-the-internet-and-dog-years-have-in-common/>>.

differently, but also occur within a temporary process, which may discourage individuals from seeking remedies.

The final and most significant reason for the importance of this research is based on how the AI Act regulates political bots. In 2021, the draft regulation¹⁶⁰ classified high-risk AI systems if they could be used in democratic processes. Only two words, *democratic process*, were included in the draft regulation, nothing more and nothing less. Until the “ChatGPT revolution”,¹⁶¹ bots had been regarded as harmless AI systems within the categorisation of the Act. In light of concerns that these two reflections from the Act would deepen the legal gap regarding political bots, it was considered crucial in 2021 to contribute this research to the literature.

As a result, the purpose of this research is to address whether political bots are regulated under the AI Act. It also explores the extent to which political bots are addressed within the EU legal framework. This thesis further aims to identify possible regulatory gaps. Where such gaps are identified, the thesis provides practical recommendations. The analysis also draws on the findings from interviews conducted with professionals in AI.

1.2. Methodology of Thesis: A Socio-Legal Analysis of Political Bots

This section describes the methodological procedures adopted for this research. The section provides a coherent account of how the research was designed, conducted, and analysed. Additionally, this chapter provides an account of the research design, strategies, and methods used to address the research questions of the thesis. A description of how the qualitative data is gathered, treated and analysed, using a socio-legal research methodology, is presented, and

¹⁶⁰ Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 152).

¹⁶¹ Marco Bassini, ‘Speech without a Speaker: Constitutional Coverage for Generative AI Output?’ [2025] European Constitutional Law Review 1, 376 <<https://doi.org/10.1017/S1574019625100771>>.

issues associated with establishing validity and trustworthiness of the study are discussed. The process of ethical approval, confidentiality, and anonymity in this research is discussed in Chapter 4.

The influence of political bots on public political discussion and their implications for democracy must be addressed in a systematic manner. For this reason, determining the suitable methodology and method for this research was essential. This research adopts a socio-legal research methodology, combining law-in-context analysis of legal documents and interviews conducted with professionals working in the field of AI. This particular methodology and method can also mean the exclusion of other possible approaches. Therefore, this decision requires a meaningful explanation within the structure of the thesis.

Accordingly, legal research can include some challenges. One of them is addressing “rapidly changing societal, political, economic, and technological contexts.”¹⁶² In *Law in Modern Society*, Galligan presents a theoretical framework suggesting that law should be more than the rules,¹⁶³ because the interplay between law and societal dynamics focus on how law evolves, serves varying purposes over time, and interacts with social classes, political goals, and movements.¹⁶⁴ Namely, academic lawyers can construct a strong tie between the legal rules and societal concerns or necessities. For this reason, a socio-legal methodology and qualitative research methodology are followed in this research to answer the research questions above.

¹⁶² Philip Langbroeck and others, ‘Editorial Methodology of Legal Research: Challenges and Opportunities’ (2017) 13 Utrecht Law Review 1.

¹⁶³ For an analysis of the Law in Society from Denis Galligan, see Reza Banakar, ‘Having One’s Cake and Eating It: The Paradox of Contextualisation in Socio-Legal Research’ (2011) 7 International Journal of Law in Context 487, 497 <<https://doi.org/10.1017/S1744552311000267>>.

¹⁶⁴ Denis Galligan, *Law in Modern Society* (Oxford University Press 2006) 27 <<https://doi.org/10.1093/acprof:oso/9780199291830.001.0001>> accessed 19 November 2024.

Socio-legal research combines different methodologies to provide a legal analysis of social phenomena. This research provides a law-in-context analysis of the AI Act, CFR, and other key EU law documents. A law-in-context analysis provides a legal framework on how political bots are used as a tool for manipulation. It also explores whether a legal path exists to strike a delicate balance between protecting fundamental rights and democracy without infringing on freedom of expression and information.

Qualitative research methodology can provide descriptive data to the researcher, whereby people's own written or spoken words might be analysed.¹⁶⁵ Since the main goal is to explore the opinions, beliefs and experience of the participants, interviews can provide detailed perspectives of personal and social lives which can then be interpreted. In this research project, data is gathered through 15 semi-structured interviews with professionals in AI from three different sub-groups: public sector professionals, company professionals who provide consultation to political parties or candidates during democratic processes, and non-governmental organisation (NGO) employees. These interviews were conducted with the ethical approval of the Maynooth University Research Ethics Committee, obtained in June 2023.

In this research project, out of the 15 interviews conducted for data collection, the majority took place online, 12 online and 3 face-to-face interviews. The semi-structured interviews included open-ended questions, allowing for flexible and free responses from the interviewees. The data gathered through open-ended questions was coded and analysed using MAXQDA. Thematic analysis was conducted to identify, analyse, and interpret themes within the data.

¹⁶⁵ Joseph A Maxwell, 'Designing a Qualitative Study.' 2 The SAGE handbook of applied social research methods 214.

This research project is funded by Research Ireland and conducted in the Centre for Advanced Networks for Sustainable Societies (ADVANCE CRT). The main goal of ADVANCE CRT is to train the next generation of researchers to provide sustainable, inclusive and socially informed technological solutions for society. In line with the aims of ADVANCE CRT, this research project is interdisciplinary and adopts a socio-legal methodology. Thus, research aims to provide recommendations to ensure sustainable societies.

1.2.1. Research Purpose

The purpose of this research is to address whether political bots are regulated under the AI Act, and if so, to what extent, from a legal perspective. If a regulatory gap is identified in the Act, the thesis aims to provide practical recommendations to address this gap, drawing on the findings from interviews conducted with professionals in AI. Additionally, the thesis aims to conduct an interdisciplinary research. The reason is that this thesis examines whether the legal framework outlined in the AI Act can be applicable to the use of political bots in democratic processes, and how the use of such bots is positioned in relation to democracy and society. Consequently, the study becomes rather complex, as it also addresses themes such as democracy, political communication, political campaigns, and elections. However, the research also aims to manage this complexity by presenting a compact yet comprehensible assessment. To achieve this, the study adopts a qualitative research methodology.

Qualitative methods are adopted to explore and explain the practical needs and requirements, as well as to provide practical recommendations. The reason to employ a qualitative approach is that it allows the researcher to construct a strong tie between legal rules and societal concerns. Additionally, this approach, the qualitative methodology, allows for exploring phenomena in their natural settings, attempting to understand or interpret them in terms of the meanings that

people bring to them.¹⁶⁶ In this research, interviews conducted with professionals in AI provided an opportunity to explore the meanings participants attach to a relatively popular phenomenon, namely the use of AI, particularly through bots, in democratic processes, as well as its implications for democracy and other related issues surrounding elections.

A preliminary literature review was conducted and revealed an extensive body of qualitative research, which highlights that AI-driven political bots may have the potential to influence democratic processes. The review further indicates that legal frameworks and practices may fall short in defending democracy against the rapidly evolving nature of digital technologies in political elections. However, following the proposal of the AI Act as a draft in 2021, and its official adoption in 2024 by the EU, it became evident that the legal framework specifically addressing AI-driven political bots remains highly limited.¹⁶⁷ Consequently, the aim of the current research is to address this gap in the literature, and to offer a unique contribution to this area. The insights derived from the research may contribute to the development of guidelines on the use of AI systems in democratic processes, and support efforts to raise ethical and legal awareness at the national level among both public authorities and relevant companies.

1.2.2. Research Questions

The research is guided by the following research questions:

- How are political bots used as tools for manipulation in political elections in Europe?
- How could the AI Act prevent political bots from being used as tools for manipulation without interfering with pluralism and freedom of expression and information?

¹⁶⁶ R Jones, 'Why Do Qualitative Research?' (1995) 311 BMJ 2 <<https://doi.org/10.1136/bmj.311.6996.2>>.

¹⁶⁷ Artificial Intelligence Act (n 40); Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (n 41); Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) 2022 [2000/31/EC].

1.2.3. Methodology

1.2.3.1. Qualitative Research Methodology

The field of law and humanities provides a credible framework to adopt a qualitative approach for legal research.¹⁶⁸ This approach prioritises human concerns and values rather than focusing on quantifiable principles of a more positivist, scientific approach.¹⁶⁹ This research adopts a qualitative research methodology. The reason for adopting a qualitative research methodology is that it provides the flexibility needed to conduct interdisciplinary research.¹⁷⁰

On the other hand, this research does not strictly follow the boundaries drawn in the literature between doctrinal and non-doctrinal approaches.¹⁷¹ It is well-established that qualitative research has a particular position within the field of legal inquiry, distinguishing between the two dominant strands of legal scholarship which are 'doctrinal' legal research and 'non-doctrinal' legal research.¹⁷² Accordingly, doctrinal research primarily asks 'what the law is' in a particular area, presenting the analysis of legal principles and their development and application. For non-doctrinal research, this approach examines the social, cultural, political, or practical dimensions of law.¹⁷³

In this thesis, the questions posed are highly relevant to law, as they explore the legal framework that the AI Act provides for political bots. Yet, the research not only focuses on 'what the law is' but also on 'what it does,' 'how it works,' and its effects on society and democratic processes. Indeed, due to the limitations of doctrinal research, in particular its

¹⁶⁸ Steven Cammiss and Dawn Watkins, 'Legal Research In the Humanities' in Dawn Watkins (ed), *Research methods in law* (Routledge 2013) 81.

¹⁶⁹ *ibid.*

¹⁷⁰ Mike McConville and Wing Hong Chui (eds), *Research Methods for Law* (Third edition, Edinburgh University Press 2024) 19.

¹⁷¹ Matthew Mitchell, 'Analyzing the Law Qualitatively' (2023) 23 *Qualitative Research Journal* 102, 104 <<https://doi.org/10.1108/QRJ-04-2022-0061>>.

¹⁷² *ibid.*

¹⁷³ *ibid.*

narrow scope and reliance on case law,¹⁷⁴ this research adopts a socio-legal approach, considering a broad range of applied social science methods.

The chapters of this thesis are structured considering these methodological approaches. The bot concept is briefly introduced in Chapter 1. The theoretical framework, which draws on Habermas's theory of the public sphere, provides an understanding of how political bots operate within democratic processes. Moreover, it explores where their activities can be situated within society, whether they belong to the public sphere, and if so, how. Chapter 2 also addressed AI governance from political bots' perspective. This assessment draws on Habermas's political public sphere theory, existing literature on political bots, and the AI governance literature. However, Chapter 2 was not a doctrinal analysis.¹⁷⁵ Rather, it was an interdisciplinary examination, drawing from various fields of the social sciences, particularly sociology and law, to analyse how technology and AI can be approached in the context of political bots.

As a result, this research is theoretically informed,¹⁷⁶ as the law-in-context approach requires a conceptualisation of the relation between law and society.¹⁷⁷ In this way, this relationship reflects the synchronic and diachronic interactions that constitute the interdependencies at the core of law's dialectical transformations.¹⁷⁸ Moreover, from the European perspective, the law-in-context approach is linked to history, economics, sociology, psychology, politics, and

¹⁷⁴ McConville and Chui (n 424) 5.

¹⁷⁵ Mitchell (n 171) 104.

¹⁷⁶ Darren O'Donovan and Darren O'Donovan, 'Socio-Legal Methodology: Conceptual Underpinnings, Justifications and Practical Pitfalls' in Laura Cahillane and Jennifer Schweppe (eds), *Legal research methods: principles and practicalities* (Clarus Press 2016).

¹⁷⁷ Seán Patrick Donlan and Lukas Heckendorn Urscheler (eds), *Concepts of Law: Comparative, Jurisprudential, and Social Science Perspectives* (Routledge 2016) 301
<<https://doi.org/10.4324/9781315573298>>.

¹⁷⁸ *ibid.*

related disciplines, and it integrates these related disciplines into a renewed form of legal scholarship.¹⁷⁹

Additionally, the research methodology relies on qualitative data which is used as “an umbrella term” and encompasses all types of unstructured data.¹⁸⁰ Sound qualitative research depends on minimising potential bias, as possible.¹⁸¹ For this purpose, in this research, open-ended questions were designed to collect data from interviewees, ensuring that no guidance or implication would cause the biased.

On the other hand, considering the potential influence of researcher on data collected and the analysis is another essential part of the analysis.¹⁸² Nevertheless, the open-ended questions were asked to minimise this effect in the research. This design of the questions allowed participants to explain what the questions made them think of, in their own structure and order, ensuring that the researcher had no influence on their responses and reflections.¹⁸³ As people tend to record as data what makes sense to them or captures their interest,¹⁸⁴ repetitive phrases and conversational fillers such as “you know” or “right?” were excluded from the analysis in this research. However, selectivity in qualitative data cannot be fully eliminated.

¹⁷⁹ *ibid* 86.

¹⁸⁰ Udo Kuckartz and Stefan Rädiker, *Analyzing Qualitative Data with MAXQDA: Text, Audio, and Video* (Springer 2019) 1.

¹⁸¹ Margaret D LeCompte, ‘Analyzing Qualitative Data’ (2000) 39 *Theory Into Practice* 146, 146 <https://doi.org/10.1207/s15430421tip3903_5>.

¹⁸² Kate Seers, ‘Qualitative Data Analysis’ (2012) 15 *Evidence Based Nursing* 2, 2 <<https://doi.org/10.1136/ebnurs.2011.100352>>.

¹⁸³ See the detailed explanation about data analysis and interview analysis in Section 4.5.3.1. Interviewing.

¹⁸⁴ LeCompte (n 181) 146.

1.2.3.2 Socio-legal Research Model

This qualitative research is supplemented by socio-legal research methodology which is also known as law in context.¹⁸⁵ Within this framework, it is essential that legal researchers demonstrate an understanding of the methodological reasoning behind their choice of methods and methodologies.¹⁸⁶ Therefore, this section briefly discusses what socio-legal research methodology entails and why it has been adopted in this study.

The research adopts a socio-legal approach, considering its intellectual advantage.¹⁸⁷ The reason is that this thesis seeks to position legal research at the centre of social sciences, thus, the 'law in context' approach has been adopted.¹⁸⁸ Accordingly, the research explores the political bots in the light of the context in which they emerged and the actors that have contributed to shaping their legal and regulatory framework. This thesis also adopts the legal analysis method, thereby providing intentional selection of data. Also, policy documents, journal articles, book chapters, blogs, and publications related to the research questions are analysed as part of this research model.

This methodology covers legal analysis of primary sources in the law such as the AI Act¹⁸⁹ and the CFR.¹⁹⁰ The legal analysis inquires as to how the EU's legal framework on AI regulates political bots in democratic processes, particularly concerning freedom of expression and

¹⁸⁵ Fiona Cownie and Anthony Bradney, 'Socio-Legal Studies: A Challenge to the Doctrinal Approach' in Dawn Watkins (ed), *Research methods in law* (1st Edition, Routledge 2013) 35.

¹⁸⁶ Darren O'Donovan and Darren O'Donovan (n 176) 4.

¹⁸⁷ Cownie and Bradney (n 185) 36.

¹⁸⁸ Selznick explains law in context as a concept that highlights the many ways in which legal norms and institutions are shaped by culture and social organisation. Also, 'law in context' is about examining "special problems a legal order faces at a given time in its history." For this reason, this research examines the legal framework of political bots within this short period, during which AI systems have begun to be regulated globally. See more Philip Selznick, "Law in Context" Revisited' (2003) 30 *Journal of Law and Society* 177, 177.

¹⁸⁹ Artificial Intelligence Act (n 40).

¹⁹⁰ Charter of Fundamental Rights of the European Union (n 39).

information. The research assesses the effectiveness of this legal framework through thematic analysis based on interviews with AI professionals.

The law-in-context approach considers legal questions from broader perspectives and integrates insights from different academic disciplines. As Mather highlights “law is not autonomous, or standing outside of the social world, but deeply embedded within society.”¹⁹¹ This is why a law-in-context approach is related to a socio-legal or law and society perspective. In this research, research methods from sociology have been applied to explore the research questions. Thus, the socio-legal research methodology facilitates interdisciplinary research.

The thesis presents findings based on qualitative interdisciplinary research. As the research questions require an analysis of how the legal framework is viewed by society, how it regulates, and how it influences society. This approach underlines how the legal framework is shaped within social structures. For this research, law in context analysis is adopted to consider broader issues and perspectives of political bots in law and society. This analysis includes the AI Act, CFR, and soft law instruments regarding democratic processes such as European Democracy Action Plan,¹⁹² The Strengthened Code of Practice on Disinformation 2022,¹⁹³ Code of Conduct for the 2024 European Parliament Elections.¹⁹⁴

¹⁹¹ Lynn Mather, ‘Law and Society’ in Robert Goodin (ed), *The Oxford Handbook of Political Science* (1st edn, Oxford University Press 2013) 289.

¹⁹² ‘European Democracy Action Plan’ (European Commission 2020) <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790>>.

¹⁹³ ‘The Strengthened Code of Practice on Disinformation 2022’ (European Commission 2022) 202 <<https://ec.europa.eu/newsroom/dae/redirection/document/87585>>.

¹⁹⁴ International Institute for Democracy and Electoral Assistance (International IDEA), ‘Code of Conduct for the 2024 European Parliament Elections’.

1.2.3.3. Other Methodologies Considered

Alternative qualitative methodologies were considered to design the research, however, some of them were not appropriate in light of the research aim and research structure. Thematic analysis is one of the closely considered alternative methodologies. The reason for considering thematic analysis is that it is used to identify recurring themes, and to organise and describe data.¹⁹⁵ In particular, thematic analysis supports the research for using the MAXQDA software program to analyse the interviews with the experts in AI.

1.2.4. Procedures for Data Capture

1.2.4.1. Document Analysis

This research adopts document analysis as a method since it is one of the valuable approaches in qualitative research methodology. Qualitative research methodology encompasses various types of ways to collect data, and document analysis is a particularly valuable one. Unlike methods requiring direct interaction between the researcher and participants, document analysis focuses on pre-existing data. This method is specifically designed to explore latent meaning in data.¹⁹⁶

Document analysis allows for the rigorous and systematic analysis of the contents of written documents. It also provides several advantages, particularly in terms of accessibility, efficacy, and timeliness. The researcher can quickly access extensive datasets thanks to increasing availability of digital research networks and databases. This is especially beneficial in studies constrained by time, such as PhD research projects, since databases facilitate engagement with

¹⁹⁵ Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology' (2006) 3 *Qualitative Research in Psychology* 77 <<https://doi.org/10.1191/1478088706qp063oa>>.

¹⁹⁶ Sharan B Merriam and Elizabeth J Tisdell, *Qualitative Research: A Guide to Design and Implementation* (Fourth edition, John Wiley & Sons 2016) 2; Hani Morgan, 'Conducting a Qualitative Document Analysis' [2022] *The Qualitative Report* 65 <<https://doi.org/10.46743/2160-3715/2022.5044>> accessed 6 March 2025.

current academic and policy debates regarding research topic. Moreover, researchers can observe how research evolves in alignment with current research and sources.

For this qualitative research, document analysis is complemented by interviews and their thematic analysis to ensure triangulation.¹⁹⁷ Thus, it allows for a more comprehensive understanding of the consistency and validity of the findings. Document analysis has been applied to legal texts, including the AI Act, the CFR, decisions of the CJEU and the ECHR, as well as related guidelines published within the EU legal framework regarding AI systems. The document analysis of these texts, along with the interviews conducted with professionals in AI has been designed to ensure triangulation of the findings of this research.

1.2.4.2. Interviewing and Transcription

To collect new qualitative data, there are many ways, such as photo elicitation, vignettes, respondent photography, diaries, observations, and interview. Qualitative interviews refer to a research method in which the researcher conducts face-to-face interviews with participants, or interviews them via telephone or the internet.¹⁹⁸ This method is preferred as it offers a time-saving and cost efficient way to explore the topic detailed.¹⁹⁹ Thus, the researcher collects data from the primary source, namely participants. Asking follow-up questions enables the researcher to engage in a deeper exploration of the research topic and to gain substantive insights.

¹⁹⁷ Triangulation helps to assess the consistency of findings and means a strategy to increase the trustworthiness of the research. To achieve triangulation in a research, researchers can apply different methods to collect information, thereby, they can confirm their findings across data sets. See more Morgan (n 196) 65.

¹⁹⁸ John W Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed, SAGE Publications 2014) 294.

¹⁹⁹ Timothy John Rapley, 'The Art(Fulness) of Open-Ended Interviewing: Some Considerations on Analysing Interviews' (2001) 1 *Qualitative Research* 303, 317 <<https://doi.org/10.1177/146879410100100303>>.

This research is designed using semi-structured interviews. The reason for this approach is that semi-structured interviews provide for a deeper understanding of participants' unique perspectives, rather than a generalised understanding of a phenomenon.²⁰⁰ Additionally, semi-structured interviews are well-suited for exploring complex social-behavioural research inquiries.²⁰¹ This interdisciplinary research project examines the AI legislative framework of the EU concerning political bots and elections from both legal and sociological perspectives, as it also involves complex social-behavioural research inquiries.

On the other hand, one key advantage of semi-structured interviews is that it allows the researcher to investigate relevant themes or ideas that may arise during the interview.²⁰² In this research, semi-structured interviews are conducted, allowing flexibility beyond a strictly defined interview structure. Follow-up questions enable an in-depth analysis of emerging and relevant themes, which are later reviewed and integrated into the findings.

The questions in these semi-structured interviews are designed to be open-ended. A semi-structured interview often consists of main open-ended questions with follow-up probing questions. This approach contrasts with closed-ended questions—such as yes/no, or multiple-choice questions—commonly used in survey instruments for quantitative analysis. However, open-ended questions provide interviewees with flexibility to articulate their answers in their own words.²⁰³ Thus, the researcher can better understand how interviewees approach the research topic and the perspectives they bring, also allowing for in-depth analysis. In this

²⁰⁰ McGrath C, Palmgren PJ, Liljedahl M. Twelve tips for conducting qualitative research interviews. *Med Teach*. 2019;41(9):1002–1006.<https://doi.org/10.1080/0142159X.2018.1497149>

²⁰¹ Omolola A Adeoye-Olatunde and Nicole L Olenik, 'Research and Scholarly Methods: Semi-structured Interviews' (2021) 4 JACCP: Journal of the American College of Clinical Pharmacy 1358, 1361 <<https://doi.org/10.1002/jac5.1441>>.

²⁰² *ibid* 1360.

²⁰³ Ruth Kircher, 'Questionnaires to Elicit Quantitative Data' in Lena Zipp and Ruth Kircher (eds), *Research Methods in Language Attitudes* (Cambridge University Press 2022) 129 <<https://www.cambridge.org/core/product/identifier/9781108867788/type/book>> accessed 6 March 2025.

research, 15 interviews with professionals in AI have been conducted as a part of this research.²⁰⁴

1.2.5. Conclusion

This study does not claim to be a doctrinal legal research. Rather, it is an interdisciplinary research that draws upon both law and sociology to address political bots from legal and social perspectives. From this framework, the research primarily adopts a socio-legal methodology, which allows for conducting interdisciplinary research. Accordingly, a law-in-context analysis is adopted as a method for assessing the legal dimensions of political bots.

The thesis builds its overall research design on two main methodological approaches: qualitative research methodology and socio-legal research methodology. Other methodological approaches have been excluded, as this research assesses a complex topic. The subject matter of this thesis, which brings together democracy, elections, artificial intelligence (AI), and bots, requires an approach multi-layered and comprehensive.

In its overall structure, the thesis places legal research at the centre of the research (Chapter 3) and utilises qualitative methods to deepen the analysis by engaging with various dimensions of the social sciences. Thanks to the qualitative research methodology, this research gathers insights from professionals in AI through semi-structured interviews on issues concerning political bots, the AI Act, and AI governance. The data are then analysed using MAXQDA software, and the findings are presented through thematic analysis. As a result, this

²⁰⁴ The details of the interview process conducted through MAXQDA are explained in Section 4.2, “Interviewing Process”, particularly in Section 4.2.1, “Interviewing”. Please see these sections for further explanation.

interdisciplinary approach enables the thesis to provide a nuanced understanding of how legal and social dimensions intersect in the governance of political bots and AI.

1.3. Structure of Thesis

This thesis consists of six substantive chapters. Chapter 1 provides an overview of the thesis, including a comprehensive explanation about methodology and structure of the thesis. Chapter 2 establishes the theoretical framework of the research. Chapter 3 examines the primary legal framework of the EU. Chapter 4 explains the analysis of interview data and presents the findings from interviews. Finally, Chapter 5 concludes the thesis by highlighting recommendations for society and identifying gaps in the academic literature for future research.

Accordingly, Chapter 1 provides an overview of the thesis, including a detailed information on thesis methodology and its structure. This chapter provides an interdisciplinary introduction to bots and political bots. In doing so, it offers a concise and coherent summary for the audience, and helps clarify the key terminology relevant to the research project. Additionally, Chapter 1 presents the reasonable argumentation for conducting a socio-legal analysis of political bots by highlighting research purpose, research questions, and the considerations behind the selected research method and methodology. Namely, it explains why comparative or quantitative research methods were not employed and discusses why the chosen methodology and methods are suitable for this study. Finally, the chapter emphasizes that, since one of the goals of the research is to propose policy recommendations, the socio-legal approach is particularly well-suited to this purpose. The chapter also introduces the data collection procedures of the research, including document analysis and interviewing. However, the detailed assessment and explanation of the interviews are provided in Chapter 4.

Chapter 2 presents the theoretical framework of this research. It draws upon Jürgen Habermas's work, particularly his 1962 book *The Structural Transformation of the Public Sphere*,²⁰⁵ and his article in 2023 "The New Structural Transformation of the Public Sphere and Deliberative Politics."²⁰⁶ This is because political bots operate within the public sphere, and the boundaries, if they still exist, between the public and private spheres play a critical role in understanding their functions in society. Pinpointing where these boundaries lie is crucial to defining the political bots under EU law and the AI Act, and for identifying any gaps in current regulatory approaches. Consequently, Chapter 2 presents conceptual and theoretical findings.

The chapter explores the blurring boundaries between the public and private spheres, highlighting how Habermas's arguments have evolved, especially in light of contemporary events such as the January 6th, 2021 US Capitol attack.²⁰⁷ It emphasizes that the formation of public opinion would be supported by a media structure that enables deliberation, not as a matter of political governance but as a constitutional imperative. Thus, this chapter outlines the theoretical framework of the thesis by considering Habermas's arguments from the article and book from the political bots' perspective.

This chapter conceptualises political bots as digital actors embedded in the public sphere. It also addresses the following questions: Are political bots the digital continuation of traditional media in electoral campaigns? Furthermore, as digitalization transforms media, what is the role of political bots in new media? In conclusion, this chapter argues that in the digital age, deliberative democracy cannot be left at the mercy of digital platforms. Instead, similar to

²⁰⁵ Habermas (n 59).

²⁰⁶ Habermas (n 145).

²⁰⁷ This example is drawn from the US, but it reflects a global process in which democracy is becoming more fragile in the face of digitalisation. Thus, this example, Capitol Attack does not distract from this research. Indeed, Habermas also refers to the Capitol Attack. *ibid* 152.

Habermas's perspective, democracy must be strengthened, not transformed, through adherence to constitutional mandates. This chapter also aims to demonstrate how political bots undermine deliberative democracy through a Habermasian perspective. In addition, political bots and their activities are examined in Chapter 2 through Habermas's theory of the distinction between the public and private spheres. Chapter 3, in turn, evaluates these activities within the legal framework established by the AI Act. Therefore, the nature and functions of political bots are summarised or revisited in those chapters accordingly.

Chapter 3 focuses on the primary legal framework of the EU, specifically addressing the research questions by examining the relevant EU regulations. The chapter begins with an exploration of how the AI Act defines AI systems and highlights their key characteristics. Then, it investigates how the AI Act regulates bots, analysing whether the requirements based on various purposes of their use such as democratic processes and general-purpose AI (GPAI).

Chapter 3 also evaluates political bots under the scope of the CFR, particularly regarding freedom of expression and information (Article 11). This evaluation is conducted in light of the European Court of Justice (CJEU). Furthermore, the chapter analyses the use of bots in relation to Article 8 (protection of personal data) and Article 7 (respect for private and family life), exploring whether the information disseminated by bots aligns with these legal protections. The chapter also discusses the free flow of information and the right to access to accurate information, raising questions such as "What constitutes accurate information, and for whom?". The chapter investigates where political bots fall within the boundaries of freedom of expression, and how the legal system defines and regulates this freedom, particularly with regard to its limits. Consequently, Chapter 3 provides legal and doctrinal findings.

Chapter 4 outlines the methodology used in this research. It highlights the use of thematic analysis, conducted through MAXQDA, and how this method contributed to the analysis and findings of the research. Also, this chapter presents the findings. It focuses on the results of the law-in-context analysis, detailing what the analysed the AI Act offer regarding political bots. These findings are based on textual analysis of the legal framework. However, the findings provide an in-depth analysis of the interviews conducted as part of this research. This chapter focuses on empirical findings derived from interview data. The main codes used in MAXQDA for data analysis include perspectives of the participants on political bots, democracy, AI definitions, ethics, EU law, the AI Act, media, and media blackout periods. The research further conducts a detailed analysis of each subgroup to identify common approaches and differences, with a particular focus on positive and negative perceptions regarding AI definitions, the implementation of EU law, the sufficiency of current regulations, and the role of media in political campaigns. The professional backgrounds of interviewees were also considered in the analysis to uncover any shared viewpoints across subgroups.

In the conclusion, Chapter 5, the contributions of this research project to sustainable digital technologies are discussed. The focus then shifts to the use of political bots in democratic processes, evaluating the adequacy of existing legal regulations in countering their manipulative effects. The conclusion identifies gaps in current practices and offers recommendations for measures that should be taken to address these issues. Additionally, specific policy suggestions are provided to mitigate the risks posed by political bots. The findings in this project are important for the policy making processes because socio-legal research analyses case law, explaining the rules that should be applied in specific situations. The conclusion also reflects on the future directions of this research, discussing how it

contributes to the existing literature on sustainable digital technologies and democratic processes.

1.4. Conclusion

Chapter 1, this chapter, outlines the foundational structure of the thesis by introducing the key concepts, scope, and structure of the thesis. The chapter began by posing how digital tools and social media dynamics challenge democratic processes. The chapter illustrates that political bots, particularly those driven by AI, are not only tools for communication but also instruments of manipulation that can influence public perception, distort political debate, and change the course of electoral processes.

Also, the chapter clarifies main research questions guiding this thesis. The research questions focus on how political bots are used as a tool for manipulation in political elections in Europe and how the AI Act could prevent political bots from being used as a tool for manipulation without interfering with pluralism and freedom of expression and information. To answer these questions, an interdisciplinary and socio-legal research approach is adopted in this research. Thus, the methodology helps to analyse the complex interaction between technology, law, and democracy. In addition, law-in-context analysis and qualitative interviews provide a robust framework to explore the intersection of legal norms, technological tools, and democratic values from the perspective of political bots.

Additionally, Chapter 1 provides a conceptual and historical overview of bots, outlining their various types and technological developments in a summarised form. This background is essential for understanding the categorisation of political bots both legally and conceptually. By introducing key terminology and framing the research within both legal and theoretical perspectives, including Habermas's theory of public and private spheres, this chapter has

prepared the audience for the more detailed analysis to follow. In short, Chapter 1 sets the scene for the thesis by outlining its objectives, theoretical background, legal context, and methodological foundation. It provides the necessary foundation for the critical analysis of legal gaps in the AI Act from the perspective of political bots in chapters that follow.

This chapter introduced the research topic and clearly outlined the purpose of the study, the research questions, and the methodological framework of the thesis. To develop the theoretical framework of the study, Chapter 2 examines Habermas's theory of the public sphere. Accordingly, the next chapter aims to deepen the theoretical understanding of how political bots operate within the public sphere.

Chapter 2: Theoretical Framework: Political Bots and the Changing Political Public Sphere

2.1. Introduction: Theoretical Framework

This chapter draws the theoretical framework of political bots with a particular focus on Habermas's public and private spheres theory. This is because Habermas first addressed the concept of the public sphere in 1962²⁰⁸ and later revisited his ideas on its structural and historical transformation in light of technological developments over time.²⁰⁹ In this respect, his theory does not approach the public sphere as a static concept, but rather recognises its continuous evolution from traditional public spaces to contemporary digital environments. Since political bots operate within the digital public sphere, Habermas provides one of the most comprehensive and applicable theoretical approaches for understanding and conceptualising this transformation. Moreover, the technological development of bots has also progressed rapidly, and they have increasingly begun to transform the public sphere itself. For this reason, Habermas's public sphere theory was considered particularly relevant as the theoretical framework of this study.

As explained in the introduction to this thesis and above, the theoretical framework builds upon Jürgen Habermas's *The Structural Transformation of the Public Sphere* (1989),²¹⁰ and further

²⁰⁸ The book was first published in German in 1962 and later translated into English in 1989. Habermas (n 59).

²⁰⁹ This book consists of three sections and also includes Jürgen Habermas's article mentioned above "Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere". For this thesis, the Turkish and English versions were carefully analysed and reviewed. See Jürgen Habermas and Ciaran Cronin, *A New Structural Transformation of the Public Sphere and Deliberative Politics* (Polity Press 2024); Jürgen Habermas, *Kamusalığın Yeni Bir Yapısal Dönüşümü ve Müzakereci Demokrasi* (in Turkish) (1st Edition, İletişim Yayınları 2023).

²¹⁰ The book was first published in German in 1962 and later translated into English in 1989. Habermas (n 59).

engages with Habermas's recent article, *Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere*,²¹¹ translated to English in 2022,²¹² which reconsiders the public and private sphere distinction in the light of digitalisation. In 1962, Habermas provides structural and historical transformation of public sphere with a comparison private spheres. As mentioned above, this approach is quite applicable to political bots since they are operating in a digital yet public sphere.

The framework developed by Habermas provides a critical perspective on boundaries between the public and private spheres. The public sphere historically emerged from the private. In 2022, Habermas revisited the concept of public sphere and addresses the new media and related industries in shaping public sphere. The essence of this reconsideration is precisely the blurring of the boundaries between the public and private spheres. However, the thesis takes the argument a step further by suggesting that almost everything once located in the private sphere has now become part of this new public sphere. The borderless structure of the networked information environment allows it to permeate and interconnect both public and private spheres.²¹³ Today's reality reflects a new mode of existence in which privacy has become something that requires immense effort to protect. At this juncture, the thesis aims to conceptualise political bots through the perspective of Habermas's private and public spheres theory, thereby, providing a theoretical foundation for exploring their legislative framework in Chapter 3.

²¹¹ Habermas (n 145).

²¹² This book consists of three sections and also includes Jürgen Habermas's article mentioned above "Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere". For this thesis, the Turkish and English versions were carefully analysed and reviewed. See Jürgen Habermas and Ciaran Cronin, *A New Structural Transformation of the Public Sphere and Deliberative Politics* (Polity Press 2024); Jürgen Habermas, *Kamusalığın Yeni Bir Yapısal Dönüşümü ve Müzakereci Demokrasi* (in Turkish) (1st Edition, İletişim Yayınları 2023).

²¹³ Claire Wardle and AbdelHalim AbdAllah, 'The Information Environment and Its Influence on Misinformation Effects' in Tina D Purnat, Tim Nguyen and Sylvie Briand (eds), *Managing Infodemics in the 21st Century* (Springer International Publishing 2023) 46 <https://doi.org/10.1007/978-3-031-27789-4_4> accessed 7 September 2025.

The present chapter explores the position of political bots in the public sphere. Subsequently, the chapter analyses whether political bots can be an extension of electoral campaigns in digital media, which have traditionally been conducted through mainstream media. It further investigates the role of political bots in new media, if any. Then, the chapter examines the mediation and automation of political communication through the framework of platform responsibility that Habermas attributes to digital platforms. Additionally, the chapter examines how political communication via new media can evolve and influence electoral campaigns and whether automation makes computational propaganda more efficient during election campaigns. Finally, it evaluates the governance of political bots, by remaining consistent with the theoretical framework throughout the analysis. Consequently, Chapter 2 aims to present conceptual and theoretical findings.

2.2. Political Bots and the Changing Political Public Sphere

2.2.1. The Position of Political Bots in the Public Sphere

Habermas assigns a central role to the political public sphere.²¹⁴ Accordingly, public sphere facilitates access to relevant information affecting the public good and ensures open, free and public debate. However, as discussed in relation to Habermas's concept of the public sphere, an ideal form of public sphere has never existed in reality.²¹⁵ Political bots seem to have the potential to be positioned at the centre of the political public sphere; however, they are not yet. This central role requires two conditions, as set out by Habermas: involving everyone in political discussions, and using deliberation as a filter.²¹⁶ Everything, including discussions,

²¹⁴ Habermas (n 145) 150.

²¹⁵ Eileen Culloty and Jane Suiter, *Disinformation and Manipulation in Digital Media: Information Pathologies* (Routledge 2021) 85.

²¹⁶ Habermas (n 145) 150.

protests, political activities, or political actors, can hold a central position in the political public sphere if they meet these conditions.

Political bots may give an impression of meeting these conditions; however, in reality, they do not fulfil them. First, political bots encourage users to attend political discussions as a result of the deliberative filter. However, these bots include only targeted users²¹⁷ in discussions, not everyone. This is because they profile individuals and target those who could be persuaded. The identification of individuals through the content they search for or access is easily achievable.²¹⁸ As highlighted in Chapter 3, web scraping, compressing massive amounts of datasets into smaller notation,²¹⁹ data analysis all serve the refinement of targeting.²²⁰ Thus, bots are more complicated than they were assumed to be in draft versions of the AI Act. Anthropomorphising is among the strategies for which bots are used in elections—they may post at irregular intervals, use inconsistent language, deliberately make spelling errors, or include trendy words and phrases.²²¹ In such a case, detecting these anthropomorphised agents that participate in public discussions is another layer of complexity, and their relation to freedom of expression and information is also addressed in Chapter 3. However, political bots, in doing so, adjust their behaviour to align with the inclusive nature of a deliberative approach that, in theory, should involve 'everyone.' When used within echo chambers, bots may not

²¹⁷ Targeted users can be individuals or candidates. According to Wagner and others, a 'target' is defined to represent a user who has been singled out by a social bot attack. See Claudia Wagner and others, 'When Social Bots Attack: Modeling Susceptibility of Users in Online Social Networks' (2012). Also, candidates or candidacy processes can be targeted 'by illegal hate speech, harassment, or impersonation efforts, including the use of deceptive manipulated media, for example manipulated images, voice recordings or deepfakes.' See 'DSA Elections Toolkit for Digital Services Coordinators Instruments, Best Practices, and Lessons Learnt' (European Board on Digital Services 2025).

²¹⁸ Wardle and AbdAllah (n 213) 46.

²¹⁹ James Muldoon, Mark Graham and Callum Cant, *Feeding the Machine: The Hidden Human Labour Powering AI* (Canongate 2024) 162.

²²⁰ In Chapter 3, Section 3.3., titled "Could the CFR Provide Further Protection Against Political Bots?", the complex activities of bots are examined through specific regulatory dimensions, along with the relevant provisions under the CFR.

²²¹ 'AI and the Audiovisual Sector: Navigating the Current Legal Landscape' (IRIS 2024) 81.

perpetuate discussion, but rather reinforce users' pre-existing thoughts. Moreover, on platforms where political bots are present, the deliberation is limited only to the number of users, meaning not everyone in society is involved — but it still works.²²²

Second, political bots can help to improve and spread the deliberation during democratic processes. However, this is an illusion, as a discussion steered by political bots lacks the characteristics of deliberation and is not genuinely deliberative. This is because the main goal for programming political bots is not reflecting diverse perspectives. Instead of fostering a dialogue, in some examples, bots contribute political public sphere through their monologues, or sometimes even through meaningless words. While it is technically possible for bots to exchange information and knowledge, such interactions are inevitably limited by the data they are trained on or have accessed. Moreover, whether the knowledge they share is unbiased remains questionable due to the lack of transparency regarding their trained datasets and how algorithms work.²²³ This highlights the danger that opaque algorithms may further intensify polarisation in societies that are already deeply divided.²²⁴ On the other hand, whether they can produce reasonable arguments in a deliberative sphere depends on how advanced their inference capabilities are. In short, the contribution of political bots to any deliberative exchange reflects the intention behind their programming, which is often narrow and potentially biased. Consequently, political bots do not advance the discussion of diverse views.

²²² Simon Hegelich and Dietmar Janetzko, 'Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet' (2021) 10 *Proceedings of the International AAAI Conference on Web and Social Media* 579, 582 <<https://doi.org/10.1609/icwsm.v10i1.14764>>; Orestis Papakyriakopoulos, 'Political Machines: A Framework for Studying Politics in Social Machines' (2022) 37 *AI & SOCIETY* 113, 121 <<https://doi.org/10.1007/s00146-021-01180-6>>.

²²³ Transparency here is closely related to explainability. Brkan interprets this as the data subject's right to be informed about the reasoning behind automated decisions, as well as under Article 22 of the GDPR. Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27 *International Journal of Law and Information Technology* 91 <<https://doi.org/10.1093/ijlit/eay017>>.

²²⁴ Dan Taylor, 'Op-Ed: The EU's Artificial Intelligence Act Does Little to Protect Democracy' *tech.eu* (14 March 2022) <<https://tech.eu/2022/03/14/op-ed-the-eu-s-artificial-intelligence-act-does-little-to-protect-democracy/>>.

In stark contrast to inclusiveness, political bots target specific users to cause echo chambers, polarisation, or to silence certain voices such as opposition groups, LGBTQ+ supporters, or anti-war activists.²²⁵ In addition, political bots convince voters to stay home, and are used to depress turnout during democratic processes. For instance, as Woolley and Monaco highlight, during the referendum on changing country's official name to North Macedonia, bots were used to call voters to boycott the referendum through coordinated hashtag campaigns.²²⁶ Moreover, Woolley and Monaco explains “manufacturing consensus” as another objective of political bots.²²⁷ To achieve this, they may dampen or amplify particular content, thereby seeking to sow confusion, amplify the harassment of political opponents, and directly influence voter behaviour.²²⁸

Political bots are already known to be used to influence individuals who remain undecided.²²⁹ A further question, however, is if bots target people who are already of one opinion. Does the bot strategy change their perspectives? Existing research proves that political bots frequently

²²⁵ Ross et al. confirm that individuals may be less willing to express their opinions publicly when they perceive that their private views differ from those of the majority. This research relies on the “spiral of silence” theory proposed by Noelle-Neumann. Accordingly, spiral of silence theory can be summarised as opinion climates are subject to social influence processes in which an individual’s readiness to express opinions publicly is influenced by their environment. See Björn Ross and others, ‘Are Social Bots a Real Threat? An Agent-Based Model of the Spiral of Silence to Analyse the Impact of Manipulative Actors in Social Networks’ (2019) 28 *European Journal of Information Systems* 394, 2 <<https://doi.org/10.1080/0960085X.2018.1560920>>.

²²⁶ Monaco and Woolley (n 3) 58.

²²⁷ *ibid.*

²²⁸ A very recent research proves that LLMs introduce statistically significant bias on all topics. Tsirtsis and others (n 146) 4.

²²⁹ Simon highlights, convincing undecided voters has been the primary strategy since at least 2019. However, it is important to note that being an undecided voter does not necessarily imply a lack of political knowledge or an absence of engagement with democratic processes. Recent research suggests that undecided voters are a heterogeneous group. They comprise both low-information voters with limited political knowledge and highly informed voters who deliberately postpone their electoral choice until later in the campaign. Thus, while many undecided voters exhibit lower levels of political awareness and are more susceptible to campaign persuasion, others remain undecided precisely because they closely follow political developments before reaching a decision. See Moran Yarchi, Gadi Wolfsfeld and Tal Samuel-Azran, ‘Not All Undecided Voters Are Alike: Evidence from an Israeli Election’ (2021) 38 *Government Information Quarterly* 101598, 1 <<https://doi.org/10.1016/j.giq.2021.101598>>; Simon (n 13) 163.

reinforce pre-existing beliefs or opinions.²³⁰ However, Zaller explains that opinion formation is shaped by information and predispositions.²³¹ Replacing an existing opinion with an opposing one is likely to meet a resistance. Again, Zaller explains this with *resistance axiom* which refers to resist inconsistent argument with the political predispositions.²³² But the resistance is more likely to occur when individuals have contextual information to perceive the relation between the message (which seeks to shape and form the opinion) and their predisposition.

It seems individuals with political awareness or political attentiveness are likely to be exposed to more political communication, while being more selective about which messages they internalise, attend to and accept.²³³ For them, politically aware individuals, the search for consistency and the presence or absence of contextual information will influence whether their existing opinions can be changed. Also, politically aware individuals, who can also be called informed voters, can translate their political preferences into a vote that best represents their interests.²³⁴

Thus, it suggests that engaging with individuals who have higher levels of political awareness, as Zaller refers, may present two challenges for political bots. First, such individuals may be

²³⁰ One of the principal tactics identified in the literature is “megaphoning”, thus, bots amplify and repeatedly spread certain narratives, messages, and content. Furthermore, Kenny et al. found that users exhibit myside bias during democratic processes. As a result, they can align with users existing views. Monaco and Woolley (n 3) 59; Ryan Kenny and others, ‘Duped by Bots: Why Some Are Better than Others at Detecting Fake Social Media Personas’ (2024) 66 *Human Factors: The Journal of the Human Factors and Ergonomics Society* 88, 88 <<https://doi.org/10.1177/00187208211072642>>.

²³¹ John R Zaller, *The Nature and Origins of Mass Opinion* (1st edn, Cambridge University Press 1992) 6 <<https://doi.org/10.1017/CBO9780511818691>> accessed 21 July 2026.

²³² *ibid* 44.

²³³ According to Zaller, politically aware citizens can reflect a tendency to fill their minds with large numbers of considerations. Then, these considerations can be relatively consistent with one another and with the citizens' predispositions. At the end, they will be more likely to be able to state their opinions, and more likely to state opinions that are ideologically consistent with their predispositions. *ibid* 52.

²³⁴ Anthony Fowler and Michele Margolis, ‘The Political Consequences of Uninformed Voters’ (2014) 34 *Electoral Studies* 100, 109 <<https://doi.org/10.1016/j.electstud.2013.09.009>>.

more likely to detect and identify automated behaviour on the platforms.²³⁵ Second, political bots have limited abilities to sustain a political discussion or consistent political engagement with politically aware users. Consequently, political bots can be more effective when targeting individuals with lower levels of political awareness, knowledge or attention, who are less likely to critically evaluate political messages or narratives.²³⁶ Additionally, changing the already established opinions of individuals with higher levels of political awareness is unlikely to be achieved through direct interaction with bots. Instead, as Woolley and Monaco argue, this may be achieved by seeking to sow confusion and amplifying the harassment of political opponents.²³⁷

Political bots have been used for manipulative purposes ever since their potential for political propaganda was realised. Therefore, rationally acceptable outcomes can theoretically be achieved through deliberative discussions during the elections. But this is not the objective of political bots. The purpose of political bots is to direct political discussions with voters who are open to persuasion in favour of candidates or political parties in a grey area by exceeding the boundaries, including legal and physical, set for traditional media. Due to the limited presence of gatekeepers, political bots may serve as virtual companions for users on political

²³⁵ Kenny and others proved that social media experience and "myside bias" could affect the identification performance. Another research, Ngo and others, also proved that sophisticated social bots, if they share users' political opinion are least likely to be verified. But again, Ryan and others also proved this less analytical reasoning ability reduces to detect bots. Thus, bot detection performance is likely to be influenced by analytical reasoning, political knowledge, and political awareness. See more Kenny and others (n 230) 88; Thao Ngo and others, 'Spot the Bot: Investigating User's Detection Cues for Social Bots and Their Willingness to Verify Twitter Profiles' (2023) 146 *Computers in Human Behavior* 107819, 7 <<https://doi.org/10.1016/j.chb.2023.107819>>.

²³⁶ This is because, as Geyikci and Yavuzylmaz highlight, free and fair electoral competition requires targeting three main groups: their core party groups, swing voters and rival voters. Also, a polarised political environment first targets mobilised core voters; second, chase swing voters during electoral processes. As a result, core party supporters can generally be regarded as reliable voters whose electoral preferences are relatively stable. By contrast, political bots seem likely to be more effective when deployed to influence undecided voters. Because their voting intentions remain open to persuasion. See more Şebnem Yardımcı-Geyikçi and Hakan Yavuzylmaz, 'The 2023 Turkish Election: A Tale of Two Campaigns and the Duel of Populisms' (2024) 24 *Southeast European and Black Sea Studies* 259, 260 <<https://doi.org/10.1080/14683857.2024.2315650>>.

²³⁷ Monaco and Woolley (n 3) 58.

matters.²³⁸ Before questioning whether the content they spread is manipulative,²³⁹ it is important to note that their purposes cannot always be described as manipulative per se, at least not according to the definition of political bots.²⁴⁰ By their definition and distinctive features from social bots,²⁴¹ they would remain harmless tools if they were never employed for manipulative aims. Yet, political bots seek to remain invisible or maintain an anthropomorphised presence by moving through the grey zones of platform responsibility.

Thus, as in Habermas,²⁴² the conditions of political public sphere are neither applicable to political bots nor valid for the platforms themselves. As a result, the proposed conditions by Habermas to identify the political public sphere fail to remain valid in digital political public sphere. Habermas also admits that this equation is lacking for the digital spheres.²⁴³

2.2.2. Are Political Bots the Digital Continuation of Traditional Media in Electoral Campaigns?

Political bots, as digital tools, are not a simply digital continuation to the traditional election campaigns which have been used in orthodox media. Electoral campaigns in the digital public sphere do not share the same dynamics as electoral campaigns in traditional media. There are four main reasons for this: the transformation of the dynamics for the formation of public opinion in the digital era, the lack of responsibility in new media, the absence of structured

²³⁸ Heung-Yeung Shum, Xiaodong He and Di Li, 'From Eliza to XiaoIce: Challenges and Opportunities with Social Chatbots' 11 <<https://arxiv.org/abs/1801.01957>> accessed 29 August 2023.

²³⁹ In Chapter 3, the legal position of manipulative content is addressed within the framework of freedom of expression and information. See sections 3.3.1. *Political Bots and Freedom of Expression* and 3.3.2. *Interrelation of Political Bots with Other Rights Under the CFR*.

²⁴⁰ In Chapter 1, under section 1.1.4. *What are Political Bots?*, the definition adopted for this research states that political bots are equipped with features to generate automated interactions with other users about politics. Alongside other purposes — such as electoral communication, reaching out to voters, explaining political party strategies, or providing general information about voting — manipulation can also be among the aims for which these agents are designed.

²⁴¹ Their distinctive features are addressed in Chapter 1.

²⁴² Habermas (n 145) 150.

²⁴³ *ibid* 153.

programming in new media, and the tendency of new media to create isolated groups rather than fostering inclusivity.

New media enable the formation of public opinion because platforms provide a freely accessible public sphere to everyone.²⁴⁴ Moreover, as highlighted by Celeste, social media platforms enabled users to become consumers and producers of online content.²⁴⁵ Thus, new media provide a more complex space where users can perform both roles at once. Such users are often referred to as “prosumers” participating in a business model referred to as “prosumption,” which captures the idea of producing while consuming.²⁴⁶ In economics as well, the traditional separation between production and consumption is not maintained, and platforms have further blurred the boundaries between these domains. From the perspective of political bots, within this business model, political bots do not only assume the dual roles of content producers and platform users, but they are also programmed to engage in targeted dissemination based on calculated predictions (computational politics) of other users' behaviours and tendencies.

While doing so, political bots may be detected and blocked by platforms or ignored by human users. For instance, human users can identify them as bots and may recognise that they are interacting with bots or simply choose not to engage with them for other reasons, resulting in little or no response or interaction. For each case, bots can become subject to platform moderation or user responses. Nevertheless, unless political bots are completely removed from

²⁴⁴ *ibid* 157.

²⁴⁵ Edoardo Celeste and others, *The Content Governance Dilemma: Digital Constitutionalism, Social Media and the Search for a Global Standard* (Springer Nature 2023) 9.

²⁴⁶ This term was coined by Alvin Toffler in 1980. It refers to processes of production and consumption simultaneously. Alvin Toffler, *The Third Wave* (W Morrow 1980); Orçun Kasap and Altug Yalcintas, ‘Commodification 2.0: How Does Spotify Provide Its Services for Free?’ (2021) 53 *Review of Radical Political Economics* 157, 163 <<https://doi.org/10.1177/0486613420924163>>.

the platforms and preventing from reappearing, they can still shape public opinion, particularly as they can be generated rapidly and at scale. Ross et al. proved that manipulative actors, such as political bots, can change the perceived majority opinion in a network, even when used in small numbers. These agents may lead real users to engage in self-censorship.²⁴⁷ Additionally, bots need to interact with platform algorithms to influence real users, as they can shape or reshape existing public opinion indirectly through content recommendation systems.²⁴⁸

On the other hand, bots can also be targeted by users. The case of Grok, the AI chatbot developed by xAI for the platform X (formerly Twitter), proved that bots can be vulnerable to manipulation, and users may influence their outputs. In May 2025, according to xAI, “unauthorised modifications” to Grok’s system prompt led the chatbot to display erratic behaviour.²⁴⁹ xAI explained that there would be a code review process for prompts. However, it seems the code review process had been “circumvented” in this incident.²⁵⁰ This modification further suggests that bots can generate offensive or provocative outputs when influenced by the user-driven data environment.

In some cases, Grok generated insulting or controversial content toward social media figures, individuals who may also be described as trolls, meaning real users who deliberately engage in aggressive, destructive or provocative behaviour. For instance, a social media figure, Furkan Bölükbaşı, known for supporting the ruling party (AKP) in Turkey, reportedly boycotted Grok after the chatbot had generated vulgar and controversial expressions directed at Bölükbaşı. This

²⁴⁷ As explained before, this tendency is not primarily due to the high effectiveness of manipulative tools, but rather relates to the Spiral of Silence. Ross and others (n 225) 8.

²⁴⁸ N Pescetelli, D Barkoczi and M Cebrian, ‘Bots Influence Opinion Dynamics without Direct Human-Bot Interaction: The Mediating Role of Recommender Systems’ (2022) 7 *Applied Network Science* 46, 13 and 14 <<https://doi.org/10.1007/s41109-022-00488-6>>.

²⁴⁹ Dan Milmo, ‘Elon Musk’s AI Firm Blames Unauthorised Change for Chatbot’s Rant about “White Genocide”’ *The Guardian* (16 May 2025) <<https://www.theguardian.com/technology/2025/may/16/elon-musks-ai-firm-blames-unauthorised-change-for-chatbots-rant-about-white-genocide>>.

²⁵⁰ *ibid.*

incident arose because of the absence of a code review process. It led Grok to generate insulting content toward some accounts, even without explicit user prompts. However, in this example from Turkey, there was an AI Retrieval Augmented Generation (RAG) technique to enable LLMs to improve outputs by fetching relevant, up-to-date information from external data sources. Additionally, Indirect Prompt Injection (IPI) was used to embed malicious instructions into external sources that an LLM can access and process.²⁵¹

These examples showed that chatbots do not always rely on broadly accepted or neutral information when generating outputs. Instead, their behaviour may be shaped by underlying data inputs and system-level configurations. Mechanisms such as code review processes are therefore critical in ensuring that outputs remain appropriate, neutral, and accurate. Overall, these examples demonstrate that chatbots can be targeted and manipulated by users, particularly in situations where safeguards such as prompt control and code review processes are insufficient or bypassed. There is a possibility that users may apply this reverse strategy to political bots in electoral processes.

For new media, this novel component of information ecosystem does not facilitate forming public opinion for two reasons: decreasing audience attention and content quality. The first reason for this is that public opinion can only be effective in the digital public sphere if it captures the attention of a broad audience. Yet, on digital platforms, as users consume content, their attention is simultaneously exploited by the platforms.²⁵² Habermas explains this tendency

²⁵¹ Dr Tugrulcan Elmas, *Grok Furkan Bölükbaşı'na Neden Küfretti? RAG ve Yapay Zekânın En Büyük Açığı (In English: Why Did Grok Swear at Furkan Bölükbaşı? What Are AI's and RAG's Biggest Security Vulnerability?)* (2025)

<https://www.youtube.com/watch?v=s65LH_Llf18#:~:text=Elon%20Musk'%C4%B1n%20X'e%20yerle%C5%9Ftirdi%C4%9Fi%20Yapay%20Zek%C3%A2%20edepsiz%20Grok%20Furkan%20B%C3%B6l%C3%BCkba%C5%9F%C4%B1'na%20k%C3%BCfretti.%20Ama%20neden?>>.

²⁵² This concept was used first by Herbert A Simon in 1960s, who identified the overload information as an economic challenge. According to Simon, attention, not information, becomes the scarce resource. In the digital age, this concept has undergone a transformation. Including the United Nations reports, global policy documents

with a long-term research which is conducted in Germany.²⁵³ According to research cited by Habermas, an individual spends only 18 minutes in a day to read digital texts,²⁵⁴ including political content.²⁵⁵

Thus, the question arises as how political bots could be influential. Even when the users do not spend their time reading digital texts, political bots may still have an impact. Papakyriakopoulos explains this with symbolic influence, which means non-verbal information, for example, stimuli like shapes or colours, may also play a role in influencing individuals.²⁵⁶ Indeed, such information can be stored in user's memory and later reactivated, retrieved, and deployed depending on new and related incoming information.²⁵⁷ Admittedly, symbolic influence is not a new phenomenon, as electoral campaigns rely on political iconography.²⁵⁸ Still, this can be seen in the colour and icon preferences of political parties.²⁵⁹

and literature discuss this concept as an economic model. Additionally, this model is detrimental to the principles of peace, justice, and strong institutions, as outlined in SDG 16 of the UN Sustainable Development Goals (SDG). Shoshana Zuboff examines how institutions meet the disruptive technologies and the erosion of them. In *The Age of Surveillance Capitalism*, Zuboff demonstrates how companies are increasingly employing attention as a commodity — extracting data from users and using it to predict and influence behaviour for profit. See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (First edition, PublicAffairs 2019); Shoshana Zuboff, 'Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization' (2022) 3 *Organization Theory* 26317877221129290 <<https://doi.org/10.1177/26317877221129290>>.

²⁵³ Habermas (n 145) 161.

²⁵⁴ In Habermas, digital text means the opposite of the printed newspapers and magazines. Even reading the shifted newspaper on the internet does not require the same intense level of attention. For this reason, digital texts could be the opposite of printed media pieces because they require less attention to read. See *ibid*.

²⁵⁵ Similar to this research, the UN report also highlights a decline in collective attention, alongside a reduction in individual attention. Accordingly, the broader social and political significance of this attention shift may still be underexamined. For the report see Chantal Line Carpentier, 'New Economics for Sustainable Development: Attention Economy' (the United Nations 2023) 5

<https://www.un.org/sites/un2.un.org/files/attention_economy_feb.pdf>.

²⁵⁶ Papakyriakopoulos (n 222) 121.

²⁵⁷ *ibid*.

²⁵⁸ Political iconography sometimes entailed the prohibition of certain colours or icons. For instance, in Turkey, following the 1980 military coup, during the referendum on the 1982 Constitution drafted and submitted by the junta, the blue ballot symbolized rejection/no, while the white ballot symbolized approval/yes. Up until the referendum date, the junta pressured the media, academics and others not to publish content in which the word 'blue' appeared. Accordingly, in the alternative notions of democracy that military juntas or authoritarian regimes seek to establish, the symbolic meanings attributed to colours and symbols become further intensified. Also, please see Section 2.2.2, "Are Political Bots the Digital Continuation of Traditional Media in Electoral Campaigns?", for a more detailed explanation of the inclusion of examples from Turkey.

²⁵⁹ Matteo Cm Casiraghi, Luigi Curini and Eugenio Cusumano, 'The Colors of Ideology: Chromatic Isomorphism and Political Party Logos' (2023) 29 *Party Politics* 463

As for political bots, the dissemination of these icons, colours, or symbols enables their amplification. This makes the stimuli unavoidably visible in the digital public sphere, even if users do not fully engage with them. Moreover, bots can have the advantages provided by platform algorithms, which are not transparent and whose functioning remains largely unknown. Nevertheless, the impact of symbolic effect is virtually impossible to measure in quantitative terms, although it persists.²⁶⁰

As people spend less time on informative content, they may comprehend and analyse such content with limited attention. Compared to attention and understanding demonstrated by audience in the era of traditional media, new media engagement may tend to be more superficial. Thus, deep analysis and discussion of opinions on new media may not form public opinion. On the other hand, public opinion formed through political bots does not attract the attention of this broad audience because the content lacks quality. Instead, it spreads and gains visibility because of the bots' organized actions, consistency in their posts, and numerical superiority. Also, the content published by political bots often consists of structured topics and answers, making them easier to detect, as bots rely on pre-set patterns.

Habermas addresses historical transformation of press and its relations with the capital and commercial activities when he frames the structural transformation of public sphere.²⁶¹

<<https://doi.org/10.1177/13540688221080539>>; Luigi Curini, Benjamin Moffitt and Mattia Zulianello, 'The Colors of the Populist Radical Right: The Strategic Use of Hue and Saturation in Party Logos' (2025) 30 *The International Journal of Press/Politics* 819, 829 <<https://doi.org/10.1177/19401612241229216>>; Antonio Pineda, Alberto Hermida and Elena Bellido-Pérez, 'Visualizing Political Communication on Spanish Social Media: An Analysis of Andalusian Political Parties' Communication on Instagram' [2025] *Visual Communication* 14703572241307305, 18 <<https://doi.org/10.1177/14703572241307305>>.

²⁶⁰ Papakyriakopoulos (n 222) 121.

²⁶¹ Jürgen Habermas (n 209) 148.

According to Habermas, media is crucial because it generates “competing public opinions.”²⁶² Unlike new media, which lacks an accountability framework, traditional media has a structured responsibility mechanism.²⁶³ New media has a revolutionary character relies on global dissolution of boundaries in space and time.²⁶⁴ However, there is an “inadequacy of the political regulation of those new media.”²⁶⁵ So, it raises the question: was old media really that responsible? The answer is: not particularly. Although not necessarily better, traditional media benefits from more established and long-standing rules and practices. At the same time, traditional media did possess an infrastructure of accountability, maybe imperfect, often ineffective, but nonetheless present, that new media largely lacks such an infrastructure. Shortly, old media had further regulatory oversight, but new media are less responsible than old media.

The analogue world widely accepts that the infrastructure of public sphere relies on gatekeeper roles. Authorial, editorial, and managerial functions are fulfilled by gatekeepers. Traditional media hires professional editors and fact-checkers, thus, it enables single-direction control and operates under legal responsibilities. Although the correction process can be slow, next day retractions can be possible within a controlled distribution system. In contrast, false information spreads rapidly and corrections rarely catch up. Also, in new media, it remains unclear who takes on these roles. Gatekeeping may also rely on crowdsourced processes.²⁶⁶

²⁶² Habermas (n 145) 157.

²⁶³ *ibid.*

²⁶⁴ Habermas explains this as follows “With this global dissolution of boundaries in space and time, these flows have simultaneously become condensed, differentiated and multiplied according to functions and contents, and have been generalised across cultural and class-specific divisions. The innovative idea that ushered in this third revolution in communications technologies was the worldwide networking of computers, as a result of which anyone could communicate from any place with anyone anywhere else in the world.” *ibid* 158.

²⁶⁵ *ibid* 153.

²⁶⁶ This method is often used to filter content, validate existing agendas, and maintain platform standards. Crowdsourcing was introduced by Jeff Howe in the early days of platforms. Howe emphasised that platforms would adopt this method as a cost-effective alternative to traditional employment, even if it was not entirely free. Today, platforms increasingly rely on unpaid user contributions under the promise of maintaining better

New media feed the users through algorithms to offer “personalised content” and capture user attention. For this reason, new media is not transparent. There is limited knowledge of who the authors, editors, or administrators of the platforms are. Similarly, it may not be known or possible to determine who is behind the political bots. Researchers analyse interactions and common signs, such as follower number, profile pictures, and response times between bot accounts to identify whether or not the accounts have worked together. In fact, the identities of individuals behind political bots can only be uncovered through legal investigations.²⁶⁷

Within an ethical governance framework, new media primarily governs content through platform terms and conditions. However, ethics are largely ignored, and even though citizen journalists are empowered to publish information to wide audiences, platforms do not provide ethical guidelines to citizen journalism.²⁶⁸ In contrast, traditional media operate within established legal frameworks, including national press councils or foundations and press ombudsmen, and adhere to formally defined ethical principles.²⁶⁹

While both traditional and new media compete for users’ limited time, they do so in different ways. Traditional media typically seeks to fill this limited time with curated content, whereas new media aims to maximise user attention and time spent on the platform, rather than ensuring

community standards. Users often voluntarily participate in fact-checking controversial content to prevent the spread of disinformation, and they typically do so without receiving any form of payment. See an example used by researcher Mohammed Saeed and others, ‘Crowdsourced Fact-Checking at Twitter: How Does the Crowd Compare With Experts?’ *Proceedings of the 31st ACM International Conference on Information & Knowledge Management* (ACM 2022) 1736 <<https://doi.org/10.1145/3511808.3557279>> accessed 7 May 2026; Jeff Howe, ‘The Rise of Crowdsourcing’ (1 June 2006) <<https://www.wired.com/2006/06/crowds/>>.

²⁶⁷ Select Committee on Intelligence United States Senate, ‘Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election Volume:2 Russia’s Use of Social Media with Additional View’ (2020) 116–XX 4 <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf>.

²⁶⁸ Jessica Roberts, ‘The Erosion of Ethics: From Citizen Journalism to Social Media’ (2019) 17 *Journal of Information, Communication and Ethics in Society* 409, 419 <<https://doi.org/10.1108/JICES-01-2019-0014>>.

²⁶⁹ Traditional media promise professional accountability, public accountability, and legal accountability. The same does not apply to new media to the same extent. This is largely due to the existence of areas (or activities) that fall outside established legal frameworks on platforms, as well as the limited attention span of audiences, which reduces the effectiveness of new media compared to observed in traditional media.

legal, ethical and accurate content it conveys. Habermas explains this with “time budget” of users.²⁷⁰ Traditional media offers structured programs daily, weekly or monthly. If the audience prefers to follow these periodic schedules, they can be exposed to the selected content by traditional media. In contrast, new media seeks to occupy as much of time of users as possible by encouraging them to spend it on the platforms. To achieve this, platforms employ various engagement strategies, including notifications, alerts and personalised prompts. Even users are inactive, platforms may attempt to draw their attention back through messages such as reminders about missed content, notifications that they have not been active for some time. Thus, audience in new media cannot simply disconnect from the platform.

The difference between new media and traditional media is also rooted in commercial pressures. The position of traditional media is attempting to compete with new media while operating under increasing commercial pressures, such as advertising profits and media elites. As a result, Habermas attempts to ground these commercial pressures in a meaningful framework through the ‘time budget’ concept, as mentioned above, which is invested in daily media consumption.²⁷¹

Accordingly, media consumption —including all media types— peaked in 2005, and has since been testing the saturation level of roughly eight hours per day.²⁷² Instead of time budget, new media prioritise users’ continuous online presence.²⁷³ However, new media, namely this new business model, also give rise to several risks. Most notably, while traditional media presents broadcast programming schedule transparently, new media users cannot predict what they will encounter on the platform. Political bots take advantage of this characteristic of new media by

²⁷⁰ Habermas (n 145) 161.

²⁷¹ *ibid.*

²⁷² *ibid.*

²⁷³ *ibid.*

spreading content aligned with trending topics or actively managing the trends; hence, they can be positioned as key actors in this process.

Another difference lies in inclusivity. Traditional media presents structured content that considers the media users' interests and educational backgrounds, thereby ensuring inclusivity,²⁷⁴ new media segregates users through algorithms and polarizes them for echo chambers.²⁷⁵ Echo chambers are formed as a result of social communication homophily.²⁷⁶ Echo chambers are defined as enclosed and bonded media spaces by Jamieson and Cappella who provided the first definition of this concept.²⁷⁷ They arise from "a dynamic group effect, where repetitive reinforcement of a singular viewpoint occurs among group members."²⁷⁸ The evidence of such echo chambers is commonly observed in social media.²⁷⁹

However, this raises an important question: does traditional media not also result in echo chambers? If so, how do traditional media-generated echo chambers differ from those generated by social media? In fact, the literature generally does not characterise these recurring patterns of media consumption in traditional media as echo chambers. Repeated consumption behaviours in traditional media, such as buying the same newspaper every day and being exposed (or preferred) to a particular ideological tendency, are generally not regarded in the

²⁷⁴ *ibid* 157.

²⁷⁵ To understand if people are in the echo chambers, it is necessary to consider both the online and offline sources they encounter. See more Amy Ross Arguedas and others, 'Echo Chambers, Filter Bubbles, and Polarisation: A Literature Review' (Reuters Institute for the Study of Journalism 2022) 10 <<https://doi.org/10.60625/RISJ-ETXJ-7K60>> accessed 7 May 2026.

²⁷⁶ Jiaying Liu and others, 'Conceptualizing Echo Chambers and Information Cocoons: A Literature Review and Synthesis of Current Knowledge and Future Directions' (2025) 34 *The Journal of Strategic Information Systems* 101904, 7 <<https://doi.org/10.1016/j.jsis.2025.101904>>.

²⁷⁷ Kathleen Hall Jamieson and Joseph N Cappella (eds), *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment* (Oxford University Press 2010) 76.

²⁷⁸ So the main motivation is to create homogeneous groups and to affiliate with individuals that share their political view. As Liu and others highlight, echo chambers result from collective reinforcement among group members. See details Liu and others (n 276) 6 and 7.

²⁷⁹ See details *ibid*.

literature as echo chambers. Instead, this type of consumption behaviour can be more appropriately defined with the “information cocoon” concept.

This is because an information cocoon arises from self-selection processes.²⁸⁰ Also, this can be explained by “selective exposure” concept.²⁸¹ This concept in traditional media refers the way that people search information to attain specific ends also avoid some results.²⁸² Namely, it refers to the tendency of individuals to seek out information that supports their preferences while avoiding opposing content. For instance, people can subscribe to newspapers, magazines or newsletters based on their preferences or research areas. They may choose specific newspapers to read viewpoints similar to their own or to follow a particular style of reporting. Thus, the audiences of particular outlets may share similar characteristics. As a result, this behaviour may not be explained by the concept of an echo chamber. Rather, it is better understood through selective exposure.²⁸³

Returning to this perspective, namely that of inclusivity, political bots interact with users by analysing their political tendencies and leveraging data scraped from their profiles on social media.²⁸⁴ This common practice of political bots highlights why they are not inclusive, rather,

²⁸⁰ Liu and others explain this concept as a metaphor. Accordingly, “users interact only with information consistent with their beliefs and fail to hear other perspectives and opposing information due to self-selection” in this information cocoon environment, See details *ibid*.

²⁸¹ Selective exposure is a theory in psychology but it is related to media and communication studies. This concept is rooted in cognitive dissonance theory from Festinger. Tsang explains Festinger’s theory as “According to his theory, individuals who encounter a counter attitudinal cognition or a cognition that goes against their previous decision will experience some sort of psychological discomfort.” See details Stephanie Jean Tsang, ‘Cognitive Discrepancy, Dissonance, and Selective Exposure’ (2019) 22 *Media Psychology* 394, 2 and 3 <<https://doi.org/10.1080/15213269.2017.1282873>>; Leon Festinger, ‘Cognitive Dissonance’ (1962) 207 *Scientific American* 93 <<https://doi.org/10.1038/scientificamerican1062-93>>; Leon Festinger, *A Theory of Cognitive Dissonance* (Reissued by Stanford Univ. Press in 1962, renewed 1985 by author, [Nachdr.], Stanford Univ Press 2001).

²⁸² Jean Tsang (n 281) 2.

²⁸³ As a direction for further research, the thesis suggests a broader analytical framework that integrates the concepts of information cocoon and echo chamber to further elaborate on this issue.

²⁸⁴ Social bots helps for the generation of personalised online news preferences and advertisements. Thus, users can be manipulated by political advertising according to their tendencies. See Samuel C Woolley, ‘Automating Power: Social Bot Interference in Global Politics’ [2016] *First Monday*

they are inherently selective in the users they engage with. Woolley and Monaco explain this through the surveillance capabilities of political bots.²⁸⁵ Surveillance refers to gathering any kind of data. According to the authors, this can occur in both passive and active forms. Passive surveillance operates silently in the background by processing users' data to predict their preferences about everything. Active surveillance, by contrast, involves direct interactions, such as boosting accounts, increasing visibility, and creating transparency around particular issues.²⁸⁶ As a result, this mode of interaction appears inconsistent with Habermas' conception of inclusivity in the political public sphere. This is because such interactions are typically a result of optimisation processes.

In conclusion, new media provides limitless possibilities for networking which also applies to political bots. Moreover, the timing, manner, and targets of political bot interactions remain unknown. This limitlessness provides an absolute and immune strengthening to political bots because their real and official influence can only be measured after electoral processes have concluded; their numbers remain unknown and their interactions are largely untraceable. As a result, while platforms represent the innovative face of new media, political bots are the new digital 'disruptors' of political campaigns conducted via these platforms.

<<https://journals.uic.edu/ojs/index.php/fm/article/view/6161>> accessed 25 February 2025; Also see Elizabeth Dubois and Fenwick McKelvey, 'Political Bots: Disrupting Canada's Democracy' (2019) 44 *Canadian Journal of Communication* PP, 29.

²⁸⁵ Monaco and Woolley (n 3) 70.

²⁸⁶ *ibid.*

2.2.3. As Digitalization Transforms Media, What Is the Role of Political Bots in New Media?

Habermas highlights that the platforms are responsible and liable for what information that they convey to users.²⁸⁷ Political bots stand in the same position as platforms. Similar to the platforms, political bots have power to form or reshape public opinion and mentalities, however they transmit it via the platforms, and as a part of organised political campaign strategy.

Political bots establish a multifaceted communicative connection through platforms, similar to the one established between platforms and their users.²⁸⁸ Moreover, political bots take advantage of the limitless possibilities for networking that allow consumers of new media to communicate with arbitrary addressees.²⁸⁹

Political bots leverage the network-friendly environment of platforms and can easily develop multifaceted communication. They usually do not interfere with spontaneously chosen topics on the platforms. Rather, political bots bring the topics to be discussed and keep them within platform trends to ensure the topic reaches all users. In this point, the main strategy of political bots can feed every user with structured forms of the content related to the topic. Namely, political bots do not contribute without prior structured forms of content or at least a prior strategy.

Besides the multifaceted communication, they can also exist on the platforms without actively taking on any role —such as author, content creator or re-posting content. The asymmetrical power relationship that exists between platforms and potential recipients can also be observed

²⁸⁷ Habermas (n 145) 167.

²⁸⁸ *ibid* 159.

²⁸⁹ *ibid*.

between political bots and other users on the platforms. Namely, political bots are basically users on the platforms, they can establish relationships that re-create power asymmetries with other users. This is because they possess advantageous capacities against real users and, therefore, they may dominate the platform environment. Through the data they are trained on, gather, and analyse, political bots operate on the platforms with knowledge about users, including whether individuals fit the profiles they target. Because one of the key AI-driven political bot activities may involve scraping²⁹⁰ and analysing open source data of the users, thus, political tendencies can be presumed to be targeted by bots.²⁹¹ By learning the operational logic of platform algorithms, they can easily transform both the content they seek to suppress and the content they seek to amplify. Consequently, they do not experience the same platform environment, feed, or information flow as real users. But, real users are already disadvantaged against platforms that collect extensive data about them, political bots may further manipulate the platform experience and redirect it towards other objectives, such as political persuasion. As a result, they re-create and deepen power asymmetries to the detriment of real users.

After the Cambridge Analytica scandal, Facebook closed its API,²⁹² which had allowed third parties to access and download user activity data from the platform.²⁹³ Scraper bots are used for web scraping. They can also be used by recruitment platforms to collect job postings or by real estate websites to compile property listings through scraping technologies. In academia,

²⁹⁰ Howard, Woolley and Calo, 'Algorithms, Bots, and Political Communication in the US 2016 Election' (n 57) 83.

²⁹¹ Basically, they are referred to as "scraper bots." When such bots are used for political purposes during democratic processes, they may be described as "political scraper bots," and they will represent another dimension of the political bot concept.

²⁹² API means "application programming interface." An API refers to the means by which one bit of software can talk to another.

²⁹³ Moreno Mancosu and Federico Vegetti, 'What You Can Scrape and What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data' (2020) 6 Social Media + Society 2056305120940703, 9 <<https://doi.org/10.1177/2056305120940703>>.

researchers also use such tools to gather data from online platforms. Also, price comparison platforms often depend on scraper bots to collect product pricing data from multiple e-commerce websites. This is because, as Bastos and Marcea define bots as “automatic posting protocols,”²⁹⁴ thus, bots can relay and retrieve content in a programmatic fashion.²⁹⁵ Namely, bots scrape data from internet sources and present in an organised manner.²⁹⁶ Mancosu and Vegetti explains web scraping as “the set of techniques to extract data from the internet.”²⁹⁷ Unlike search engines, these activities often target specific type of information and work intensively on particular websites.²⁹⁸

However, an important concern arises because bots may scrape publicly accessible data without explicit permission.²⁹⁹ One response to this issue is the Robots Exclusion Protocol (REP).³⁰⁰ This protocol relies on a standardised text-based system, commonly known as “robots.txt,”

²⁹⁴ Marco Bastos and Dan Mercea, ‘The Public Accountability of Social Platforms: Lessons from a Study on Bots and Trolls in the Brexit Campaign’ (2018) 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180003, 2 <<https://doi.org/10.1098/rsta.2018.0003>>.

²⁹⁵ Scraper bots operate using pre-defined scripts. They locate predefined elements and collect them into usable formats like spreadsheets or databases. They analyse and parse webpage structures, including HTML and CSS, to identify and extract desired data. See details Jaebeom You, Kisung Lee and Hyuk-Yoon Kwon, ‘DeepScraper: A Complete and Efficient Tweet Scraping Method Using Authenticated Multiprocessing’ (2024) 149 *Data & Knowledge Engineering* 102260, 2 <<https://doi.org/10.1016/j.datak.2023.102260>>.

²⁹⁶ Scraper bots operate using pre-defined scripts. They locate predefined elements and collect them into usable formats like spreadsheets or databases. They analyse and parse webpage structures, including HTML and CSS, to identify and extract desired data.

²⁹⁷ Accordingly, this method ranges from manually downloading the data by copy/pasting information from web pages to fully automated routines of data extraction. Mancosu and Vegetti (n 293) 2.

²⁹⁸ They are referred to as “scraper bots.” When such bots are used for political purposes during democratic processes, they may be described as “political scraper bots,” and they will represent another dimension of the political bot concept.

²⁹⁹ In 2022, Clearview AI was fined more than £7.5 million by the UK Information Commissioner’s Office (ICO) for unlawfully storing facial images. The French SA and Italian SA also fine Clearview AI. Diana Kwon, ‘Web-Scraping AI Bots Cause Disruption for Scientific Databases and Journals’ (2025) 642 *Nature* 281, 282 <<https://doi.org/10.1038/d41586-025-01661-4>>; Chris Vallance, ‘Face Search Company Clearview AI Overtakes UK Privacy Fine’ *BBC News* (18 October 2023) <<https://www.bbc.com/news/technology-67133157>>; ‘Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million’ *European Data Protection Board* (10 March 2022) <https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en>; ‘The French SA Fines Clearview AI EUR 20 Million’ *European Data Protection Board* (October 2022) <https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en>.

³⁰⁰ Ignoring these protocols may result in several consequences. Websites ban the server’s IP address, trigger repeated CAPTCHA verifications to prevent scraping activities, or initiate legal action against the scraper.

which is located in a website's root directory.³⁰¹ It instructs automated bots on which parts of a website they are allowed to access, index, or ignore. Therefore, the effectiveness of data collection depends on the prevailing policy regarding crawling bots.³⁰² As a result, political bots may function as political scraper bots during democratic processes. They can collect specific forms of data, such as addresses, political tendencies of individuals, and opinions on issues relevant to electoral processes or political campaign strategies, for example, views on investment in national defence sector, or civil status-related matters. Such information may enable political bots to determine which real users or user profiles they should interact with.

On the other hand, political bots exist precisely because of the transformative characteristics of new media. However, political bots are among the disruptive actors of the permeable public sphere that is provided by new media. Thanks to relatively inclusiveness of new media, every voice can be heard, which is appealing, — yet when it comes to political bots, it is questionable whether the voices of political bots are even meant to be heard. This uncertainty, as Bassini has explored, derives from the unclear constitutional status of content generated by AI systems.³⁰³ In the case of political bots, this raises a question: what would be the implication for freedom of expression if bot speech is restricted or prevented from being heard?

Over the past decade, one of the main concerns in the EU's digital policy agenda has not necessarily been AI-generated illegal content, but rather its capacity to spread disinformation.³⁰⁴ So even though bots may fall under certain legal definitions about deep

³⁰¹ These bots often disregard “robots.txt” guidelines and may attempt to bypass rate limits or security controls. Also, in 2010, Facebook prohibits automated data collection without explicit permission, there is still evidence that software continues to scrape Facebook data even after the closure of its API. Mancosu and Vegetti (n 293) 6.

³⁰² It is also possible to use “screen scraping” methods. This method is explained as automatically downloading and parsing the content on display of internet pages to obtain a usable dataset. For “Limitations of Screen Scraping” see *ibid* 2.

³⁰³ Bassini (n 161) 2.

³⁰⁴ *ibid* 3.

fakes, their potential to spread inaccurate or misleading content places them in a controversial legal gap -or grey space- when weighed against freedom of expression. In Chapter 3, this legal ambiguity surrounding the “voice” of political bots is further explored. Returning to Habermas’s framework, the question is whether the rationality and quality of media content in public discourse can be considered as an achievement for democratic deliberation.

Habermas emphasises that a significant difference between social media and the mass media is the content quality. The relevant information and knowledge are provided by the gatekeepers of mass media to form public opinion in political public sphere. This is why the roles of gatekeepers are crucial —yet, this role is absent on platforms.³⁰⁵ From this perspective, political bots intensify this challenge by exposing users to political discussions that lack depth, quality, and intensity. Mostly they introduce communication noise,³⁰⁶ for instance, by sending thousands of messages, they cause reverberation.³⁰⁷ This might be seen as an ineffective way to draw attention or form political public opinion; however, scalability, speed, and persuasiveness make this strategy impactful. Moreover, political bots carry out this strategy through social media by taking advantage of their capability to adopt complex and adaptive interaction patterns.³⁰⁸

As a result, Habermas highlights that the use of new media comes at a cost, one that is likely to remain until society learns how to use it wisely. Such a cost exists as long as users lack self-empowerment in terms of digital literacy. In other words, in an era where everyone is a potential author,³⁰⁹ users are expected to be able to read—that is, to acquire digital literacy. Without this,

³⁰⁵ Habermas (n 145) 160.

³⁰⁶ Mairieli Wessel and others, ‘The Power of Bots: Characterizing and Understanding Bots in OSS Projects’ (2018) 2 Proceedings of the ACM on Human-Computer Interaction 1, 10 <<https://doi.org/10.1145/3274451>>.

³⁰⁷ Hegelich and Janetzko (n 222) 582.

³⁰⁸ Papakyriakopoulos (n 222) 113.

³⁰⁹ Habermas (n 145) 161.

there are consequences to be paid, and those costs may not remain solely individual. Even when digital literacy and self-empowerment are present, they may still not be sufficient on their own. For instance, would it be possible to avoid paying this cost despite the numerical superiority, dynamic and swift operations and AI-driven, organised nature of political bots? Yet, despite these characteristics of political bots —whose exact influence on different countries remains vague— is the cost merely learning how to use new media wisely?

Habermas concludes at the end of the article that the platforms should be responsible and liable.³¹⁰ This conclusion can also be extended to suggest that platforms should also be primarily responsible for the information and knowledge spread by political bots. Accordingly, political bots can function as sub-platforms or micro-platforms³¹¹ within platforms, expected to be responsible solely for the content they share and accountable only to the same extent as regular platform users.³¹² Political bots, like other platform users, can be considered independent and self-responsible users. Unlike human users, they can navigate the new media better, even skilfully. Their unexpected interactions can accelerate to spread the content, thus, they can influence depth and density of discussions as trending topics on platforms. However, the content remains unstructured due to the absence of editorial filters.³¹³ This is because emancipatory promise of new media and its egalitarian-universalistic ideal of bourgeois public sphere.

³¹⁰ *ibid* 167.

³¹¹ According to Hutchinson, micro-platformisation as a process reflects “the continual fragmentation of social media platforms.” Hutchinson approaches this issue primarily from the perspective of digital activism. However, this characteristic of social media fragmentation overlaps with the fragmentation of the digital public sphere. This research argues that political bots function as micro-platform actors that contribute to the fragmentation of social media environments. In developing this argument, the research draws on the analysis of the fragmented public sphere from Habermas. Jonathon Hutchinson, ‘Micro-Platformization for Digital Activism on Social Media’ (2021) 24 *Information, Communication & Society* 35, 11 <<https://doi.org/10.1080/1369118X.2019.1629612>>; Habermas (n 145) 146.

³¹² According to Habermas, “platforms provide a multifaceted communicative connection open to networking.” This approach is applied and analysed with political bots in mind. Habermas (n 145) 159.

³¹³ Habermas finds the new media as the technically and organisationally highly complex the system. According to him, this system requires a professionalised staff that plays the gatekeeper role. *ibid* 157 and 159.

At a very basic level, sub-platforms can be defined as parts of a larger platform. More specifically, Navon and Noy define sub-platforms as “distinct communication channels which, while operating under the roof of a single social media platform, possess crucially different affordances, and as a result allow different social dynamics.”³¹⁴ For instance, various tools on platforms can be considered sub-platforms, such as Groups, Pages, Messenger, or user profiles on Facebook.³¹⁵ Similarly, YouTube channels, as part of a larger platform, may function as sub-platforms. In such spaces, audiences are often composed of individuals who share similar interests. Therefore, users display certain profile similarities. Members of these channels or communities may also develop their own jargon, interaction patterns, and group-specific norms.

Political bots may similarly operate across different platforms, such as X, Instagram, TikTok, or Facebook.³¹⁶ The choice of platform is closely connected to the characteristics of the targeted audience, as different platforms tend to attract different demographic groups and voter profiles.³¹⁷ For example, the audiences targeted on Facebook or X may significantly differ in terms of age range and online behaviour from those targeted on TikTok.³¹⁸ Accordingly, political bots may strategically adapt their activities, communication styles, and content

³¹⁴ Sarit Navon and Chaim Noy, ‘Conceptualizing Social Media Sub-Platforms: The Case of Mourning and Memorialization Practices on Facebook’ (2023) 25 *New Media & Society* 2898, 2899 <<https://doi.org/10.1177/14614448211035769>>.

³¹⁵ For details and case study see *ibid.*

³¹⁶ Research conducted in Ireland shows that messaging applications (WhatsApp, Telegram, Snapchat) are the least used for forming opinions. Robert Brennan and Rabhya Mehrotra, ‘What Media Sources Did People Use & Trust before Voting in 2024 General Election?’ *RTE* (5 June 2025) <<https://www.rte.ie/brainstorm/2025/0605/1516628-national-election-and-democracy-study-media-use-trust-general-election-2024/>>.

³¹⁷ Brian O’Donovan, ‘One-in-Five Voters Changed Ballot Choices Based on Social Media Posts - Survey’ *RTE* (28 May 2024) <<https://www.rte.ie/news/ireland/2024/0522/1450493-election-social-media/>>; Sayeh Yousefi, Ben Tappin and Jens Madsen, ‘How AI Is Shaping Elections’ (*LSE Blogs*, 8 May 2026) <<https://blogs.lse.ac.uk/politicsandpolicy/how-ai-is-shaping-elections/>>.

³¹⁸ For a brief assessment of different studies, see ‘How Different Age Groups Are Using Social Media 2026’ *Target Internet* <<https://targetinternet.com/resources/how-different-age-groups-are-using-social-media-2024/>>.

dissemination practices to the specific social dynamics and user demographics of each platform.³¹⁹ They can operate collectively in “swarms” to support a particular ideology, candidate, or political agenda.³²⁰ This enables political bots to act as coordinated communities by developing specific profiles, shared communication patterns, and distinctive jargon or terminology, including particular hashtags or slogans.³²¹ Consequently, they may become effective in creating a sense of collective identity and producing shared narratives and content.

As bot networks, bot interactions with one another and with human users may generate a new form of digital culture and political communication, often characterised by political propaganda and disinformation. In doing so, through both human–bot and bot–bot interactions, they may establish relatively self-enclosed communication ecosystems that become increasingly detached from the broader flow of the platform.³²²

Furthermore, political bots may take advantage of the opaque characteristics of the algorithms in platforms. Namely, political bots can use algorithms to increase their content visibility through trending topics and coordinated amplification strategies. By artificially promoting

³¹⁹ An article states that advertisements on Facebook and Instagram are highly popular among political parties across EU countries. Thus, political bots may also be expected to contribute to the dissemination of these advertisements and to adapt advertising content according to targeted groups. See research Cornelius Erfort, ‘Targeting Voters Online: How Parties’ Campaigns Differ’ (2024) 92 *Electoral Studies* 102872, 3 <<https://doi.org/10.1016/j.electstud.2024.102872>>.

³²⁰ Robert Booth, ‘Experts Warn of Threat to Democracy from “AI Bot Swarms” Infesting Social Media’ *The Guardian* (22 January 2026) <<https://www.theguardian.com/technology/2026/jan/22/experts-warn-of-threat-to-democracy-by-ai-bot-swarms-infesting-social-media>>.

³²¹ A study examining Japan’s 2014 General Election, titled Political Bots, Right-Wing Internet Activism, and Prime Minister Shinzō Abe’s Hidden Nationalist Agenda, states that: “Judging from the topics of the Tweets and also the netto uyo-like jargon and racist terminology as well as the names of many fake accounts, we argue that it was most likely Internet right-wingers who operated the botnets to send these Tweets.” Examples from outside the EU have also been included in this thesis because the organised use and detection of botnet activities during democratic processes has become an increasingly common practice over the last decade. These examples are important as they demonstrate how political bot strategies can be detected and how their characteristics can be identified. Accordingly, they also illustrate the feasibility of conducting further technical research on political bots. Fabian Schäfer, Stefan Evert and Philipp Heinrich, ‘Japan’s 2014 General Election: Political Bots, Right-Wing Internet Activism, and Prime Minister Shinzō Abe’s Hidden Nationalist Agenda’ (2017) 5 *Big Data* 294, 304 <<https://doi.org/10.1089/big.2017.0049>>.

³²² Habermas describes this, new media, as “a mode of semi-public, fragmented and self-enclosed communication.” Habermas (n 145) 146.

particular topics into trending lists -trend topics-, they may effectively create their own communicative spaces within the platform. At the same time, political bots frequently emerge only during specific periods, particularly during elections. Political bots can be sleeper bots and they may act like normal users for extended periods.³²³ Because of the temporary,³²⁴ adaptive, and fast-moving nature of political bots further aligns with the characteristics of micro-platforms.

Moreover, as mentioned above, bot armies operating in swarms may create the appearance that large numbers of users support a particular opinion, candidate, or political party.³²⁵ In this sense, political bots can generate an artificial image of a large and coherent supporter community. These networks enable political bots to employ consistent strategies while also functioning as relatively closed micro-publics. So, political bots operate as micro-platforms.

The functioning of political bots as sub-platforms or micro-platforms raises significant concerns regarding their responsibility. As Habermas argues, platforms facilitate the acceleration and multiplication of unexpected contacts, enabling the circulation and intensification of unpredictable forms of discourse, thereby fundamentally transforming public communication.³²⁶ Unlike traditional media, platforms enable multifaceted communicative connection forms. In traditional media, communication generally operates through a one-way and linear relationship between broadcasters and potential recipients, namely anonymous audiences consisting of readers, listeners, or viewers.

³²³ Doshi and others (n 32) 16.

³²⁴ José Van Dijck, 'Tracing Twitter: The Rise of a Microblogging Platform' (2011) 7 *International Journal of Media & Cultural Politics* 333, 333 <https://doi.org/10.1386/macp.7.3.333_1>.

³²⁵ Ratkiewicz and others (n 12).

³²⁶ For Habermas, the revolutionary character of new media does not merely lie in the expansion of media options. Rather, it reflects a profound structural rupture: from the inscription of expression onto paper, to the spread of print, and now to electronic digitalisation, where expression has become separated from printed text through binary-coded systems. See more Habermas (n 145) 158 and 159.

By contrast, communication within new media environments is established through decentralised interactions between platforms and users. This communication is facilitated by largely unregulated content flows because professional filters are lacking.³²⁷ Moreover, these environments provide spaces that are open to network-building among users. Individuals can come together around spontaneously selected topics. In principle, participants are equal and individually responsible for their own contributions.³²⁸ However, political bots do not engage in genuinely spontaneous participation, they have an agenda.³²⁹ Consequently, this is precisely the point at which political bots diverge from ordinary platform users operating within supposedly equal communicative environments.

From the perspective of Habermas, the question of political bots' responsibility must primarily be addressed at the level of platforms. The political bots interfere with pluralism, right to access accurate and objective information, the platforms are responsible as information is mediated via their channels. For instance, users can be directed not to a trustworthy source which follows journalism principles, instead, to an almost identical misleading one. Political bots can obstruct to access a reliable information through dominance of the platforms. Nevertheless, responsibility must ultimately be attributed to the platforms. By accelerating the proliferation of unexpected contacts, they act within the global network as intermediaries 'without responsibility', thereby altering the character of public communication itself.³³⁰

³²⁷ *ibid* 159.

³²⁸ *ibid*.

³²⁹ Further discussion regarding periodically political operation see. Doshi and others (n 32).

³³⁰ Habermas (n 145) 159.

On the other hand, when political bots engage in targeted interactions with users, the platform has a responsibility that either lacks or fails to deploy, the technical capacity to detect and mitigate such targeting patterns. Platforms should be designed in a way that does not undermine users' trust in the quality of information. Moreover, platforms not only profoundly transform the very character of public communication, but also reconfigure it into a new business models competing with traditional editorial actors.³³¹

Yet, in line with Habermas's emphasis on platform accountability, political bots can be held responsible to the same extent as human users. The basis of political bots' responsibility relies on their expressions on platforms. This is because, as Habermas notes, new media technologies promised to lend everyone a "publicly perceptible voice."³³² By contrast attributing direct responsibility to the programmers behind the political bots would not be meaningful. The reason is that, in line with Bassini's argument,³³³ AI-driven political bots can deviate from the original input provided by programmers and generate outputs with a degree of 'autonomy'.

In parallel with the conclusion reached by Habermas, political bots contribute to the fragmentation of the public sphere and the dissolution of boundaries between public and private spheres. This is because political bots, much like other disruptive agents, undermine the integrative power of political public spheres formed by traditional media. Habermas's perspective of the fragmentation tendencies of the public spheres and the dissolution of boundaries due to limitless communication networks can be recalled. However, in reality, the integrative political public spheres presented by unorthodox media had long been compromised

³³¹ Bassini (n 161) 6; Lidia Dutkiewicz and others, 'Artificial Intelligence and Media' in Nathalie A Smuha (ed), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (1st edn, Cambridge University Press 2025) 283 <<https://doi.org/10.1017/9781009367783.018>> accessed 6 September 2025.

³³² *ibid* 159.

³³³ Bassini (n 161) 14.

by power asymmetries, profit motives, and dependence on advertising revenues. Nevertheless, it continued to operate with the belief that journalism is one of the pillars of democracy, guided—albeit not always consistently—by journalistic ethics and its principles.³³⁴

These two developments create dynamics that stand in direct contrast to the inclusive public sphere established by traditional media. As a result, political bots not only erode the political public sphere but also deepen its fragmentation, further weakening its inclusive role. This is because political bots, by acting collectively,³³⁵ are fully aware of the power of this inclusiveness and use this power to target platform users one by one. In doing so, they dominate the digital public sphere with the content they disseminate. This domination—due to the intensity, incoherence, and aggressiveness of political bots—can reach a point where it overwhelms the platforms themselves and gradually drives human users away, either from the platforms entirely or toward alternative platforms. But democratic engagement is not confined to the digital public sphere. At the same time, political communication has been transformed and is increasingly mediated through digital platforms. This transformation highlights the potential of political bots to distort online environments to the point where they weaken, rather than support, authentic democratic engagement.

³³⁴ However, Woolley highlights that journalists, as a group and as individuals, are among the primary targets of computational propaganda, which is used against them. See details Woolley (n 53) 138.

³³⁵ Forelle et al. define this collective tactic as “robotic lobbying.” Michelle Forelle and others, ‘Political Bots and the Manipulation of Public Opinion in Venezuela’ (arXiv, 2015) 6
<<https://doi.org/10.48550/ARXIV.1507.07109>> accessed 19 October 2025.

2.3. Mediation and Automation of Political Communication

In its early stages, the Internet could be seen as a democratizing force, offering an expansive sphere for the practice of freedom of expression and the right to access information.³³⁶ However, as Keller and Celeste highlight, this praised democratic force of the internet is irremediably fading, as digital tools have increasingly jeopardised both institutions and individual rights.³³⁷ Indeed, the governance of the new digital spheres involved mediated and loosely regulated spaces.³³⁸ By contrast, the traditional boundaries and governance structures of the analogue society are largely consolidated and open to the gradual integration of new practices. The historical background of this difference, as Habermas also notes, lies in the separation between the private and the public realms: it took centuries, alongside economic and social transformations, for the distinction between *oikos* and *polis* to be fully realized.³³⁹ In the digital sphere, however, developments are advancing so rapidly—escalating like a snowball—that achieving synchronized integration, governance, and mediation within this new environment proves to be extremely difficult.

Similarly, political communication has shifted from traditional media to new media. It is conducted within social media platforms, a strategically significant manoeuvring space where automation is used and influences electoral campaigns and results. As Habermas emphasises, publishing and disseminating content on social media is responsibility of platforms. However, due to the significance and fragility of democracy, assigning this responsibility to a single actor would be inadequate.

³³⁶ Clara Iglesias Keller and Edoardo Celeste, 'Editorial | Editorial' (2019) 5 *Revista Publicum* ii, iii <<https://doi.org/10.12957/publicum.2019.47306>>.

³³⁷ *ibid* iv.

³³⁸ As Chapter 4 highlights, professionals in AI highlights there is already an excessive amount of regulation.

³³⁹ The rise of early finance and trade capitalism marked a pivotal change in the economy, which shifted its focus from *oikos* to future institutionalized economic area, *polis*. The economy had shifted away from the *oikos*; in fact, home-domestic economic activities had become integrated into the economy of the *polis* (public domain). Habermas (n 59) 14–20.

2.3.1. The Evolution of Political Communication and Influence on Electoral Campaigns

Digital information systems have emerged in response to transformations in economic institutions and structures that determine industrial dynamics.³⁴⁰ Over time, these systems have become central to modern businesses, and political election processes are no exception. One of the most significant consequences of this transformation is the internet's—and by extension, digital platforms'—role in extending and pluralizing the public sphere.³⁴¹ Among many effects of digital information systems, it has notably reshaped political communication and influence.

As a reflection of this transformation, companies specializing in political campaigns—providing services such as campaign organization, management, social media visibility, social media campaigns and election strategy—have long operated in support of candidates, parties, or political movements online. With the proliferation of the World Wide Web across many countries, digital political campaigns have become a prominent feature of elections,³⁴² altering the way political messages are disseminated and shaping voter engagement in many ways. The increasing reliance on digital information systems has further transformed electoral processes by moving them partly away from traditional broadcast media and embedding them within digital social media platforms. As a result, political communication and influence have been radically reshaped by platforms.

³⁴⁰ According to Ernst, Digital information systems (DIS) are electronic systems that integrate software and hardware to enable communication and collaborative work. See Dieter Ernst and Saskia Sassen (eds), 'The New Mobility of Knowledge: Digital Information Systems and Global Flagship Networks' *Digital Formations: IT and New Architectures in the Global Realm* (Princeton University Press 2005) <<https://doi.org/10.1515/9781400831616.89>> accessed 27 February 2025.

³⁴¹ Peter Dahlgren, 'The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation' (2005) 22 *Political Communication* 147 <<https://doi.org/10.1080/10584600590933160>>.

³⁴² Martin Moore and Damian Tambini, *Regulating Big Tech: Policy Responses to Digital Dominance* (First edition, Oxford University Press 2022) 198.

Political communication is a kind of attempt aimed at engaging voters or mobilizing supporters as part of a political election campaign. According to Howard *et al*, “political communication is a process of using information, technology, and media”³⁴³ for the benefit of power. However, the dissemination of information and the mechanisms of democratic discourse have radically changed since the rise of online social media platforms.³⁴⁴ As Gillespie emphasised, platforms constitute public discourse.³⁴⁵ Moreover, political bots have led to a significant transformation in election campaigns and political communication.

2.3.2. Platforms’ Responsibilities from the Perspective of Political Bots

The platforms³⁴⁶ like Facebook, Discord, Instagram and X, WhatsApp, Telegram have fundamentally changed political communication in the last decades in many countries.³⁴⁷ Since the platforms serve as intermediaries in the dissemination and distribution of the content which has been shared during elections, Habermas gives the responsibility to platforms for this process.³⁴⁸ Indeed, platforms are expected to act responsibly to be vigilant, transparent and unbiased when addressing threats against their users.³⁴⁹ On the other hand, the spread or

³⁴³ Howard, Woolley and Calo, ‘Algorithms, Bots, and Political Communication in the US 2016 Election’ (n 57).

³⁴⁴ Bessi and Ferrara (n 17).

³⁴⁵ Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018) 22.

³⁴⁶ According to Helberger et al., platforms are defined as “socio-technical architectures that enable steer interaction and communication between users through the collection, processing, and circulation of user data.” Natali Helberger, Jo Pierson and Thomas Poell, ‘Governing Online Platforms: From Contested to Cooperative Responsibility’ (2018) 34 *The Information Society* 1, 2 <<https://doi.org/10.1080/01972243.2017.1391913>>.

³⁴⁷ Transformations in political communication are closely intertwined with the rise of platform economies, as the emerging platform economy generates new dependencies and hierarchical structures. See more José Van, ‘Platform Mechanisms’ in José Van Dijck, Thomas Poell and Martijn De Waal, *The Platform Society* (1st edn, Oxford University Press New York 2018) <<https://academic.oup.com/book/12378/chapter/161973335>> accessed 20 October 2025; Also see Sebastian Stier and others, ‘Election Campaigning on Social Media: Politicians, Audiences, and the Mediation of Political Communication on Facebook and Twitter’ (2018) 35 *Political Communication* 50, 50.

³⁴⁸ Habermas (n 145) 167.

³⁴⁹ Onur Varol, ‘Should We Agree to Disagree about Twitter’s Bot Problem?’ (2023) 37–38 *Online Social Networks and Media* 100263, 1 <<https://doi.org/10.1016/j.osnem.2023.100263>>.

removal of just a single content can significantly impact the course of an entire election process. Therefore, platforms can take two actions about the content: removal or filtering.

In February 2024, tech companies came together in Munich to emphasize their responsibilities regarding the elections taking place that year.³⁵⁰ However, as Gillespie has previously pointed out, while platforms are vocal about the content they make available, they rarely disclose how much content has been removed.³⁵¹ Gillespie describes platforms as “algorithmically managed visibility machines”.³⁵² While the platforms promise visibility for users, they simultaneously pose risk of invisibility as well.³⁵³

Accordingly, users risk content removal if they allegedly violate community standards, and this approach is often challenged from a freedom of expression perspective, however, widely implemented in autocratic regimes (e.g., Turkey).³⁵⁴ On the other hand, filtering is considered a less invasive approach, as it prevents certain content from spreading or being seen by other users. Moreover, in 2016, Zuckerberg explicitly declared that Facebook was not a media company, thus, this statement makes clear that the company sought to avoid the burden of social and legal responsibilities. At precisely the point where Habermas argues that platforms must take responsibility, it becomes evident that companies have resisted assuming such obligations from the very beginning.

³⁵⁰ ‘A Tech Accord to Combat Deceptive Use of AI in 2024 Elections - (Proposed for Public Signature and Announcement by Technology Companies at the Munich Security Conference on February 16, 2024)’ <[³⁵¹ Gillespie \(n 345\) 5.](https://www.aielectionaccord.com/#:~:text=This%20accord%20seeks%20to%20set,with%20their%20own%20policies%20and>.”</p></div><div data-bbox=)

³⁵² *ibid* 178.

³⁵³ *ibid* 179.

³⁵⁴ See Yaman Akdeniz and Kerem Altıparmak, *Internet: Restricted Access: A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (IMAJ Yayinevi & IHOP 2008).

From Habermas's perspective, this represents platforms taking on their expected responsibility by intervening in some content to protect "discursively informed" users.³⁵⁵ However, in the 2024 US elections, claims that X's algorithms under Elon Musk's control support the Trump campaign have once again brought platform accountability into question.³⁵⁶ On the other hand, from the perspective of EU legislation, not being a voter in a particular election cannot justify exposure to biased algorithms while accessing the information.

Mediation was initially framed as a model of communication without intermediaries, however, all platforms impose rules, to some degree.³⁵⁷ Additionally, as Gillespie noted in 2018, the term 'platform' remains a 'slippery term'³⁵⁸ since technology rapidly alters their structure, fostering both centralization and decentralization. While legal frameworks attempt to manage this ambiguity by using broad or "slippery" terms, this approach deepens legal uncertainty and grants companies room to sidestep accountability. It seems that even though platforms are global players and rank among the largest and most profitable companies in the world, there are no global standards governing them, and they also tend to avoid regional regulations.³⁵⁹

³⁵⁵ Richard Foster, 'Review: A New Structural Transformation of the Public Sphere and Deliberative Politics by Jürgen Habermas' (26 August 2024) <<https://oxfordpoliticalreview.com/2024/08/26/review-a-new-structural-transformation-of-the-public-sphere-and-deliberative-politics-by-jurgen-habermas/>>; Also see Iva Nenadić, 'Unpacking the "European Approach" to Tackling Challenges of Disinformation and Political Manipulation' (2019) 8 Internet Policy Review 2 <<https://policyreview.info/node/1436>> accessed 19 October 2025. Nenadić conveys this concept through the example of people who felt "ill-informed," particularly in Brexit Britain, in relation to the campaign preceding the European Union (EU) membership referendum.

³⁵⁶ Some users prefer to leave the platform during these discussions.

³⁵⁷ Gillespie (n 345) 5.

³⁵⁸ *ibid* 18.

³⁵⁹ Ulrike Reisach, 'The Responsibility of Social Media in Times of Societal and Political Manipulation' (2021) 291 European Journal of Operational Research 906, 912 <<https://doi.org/10.1016/j.ejor.2020.09.020>>; META, Newsroom for Europe, Middle East and Africa, 'Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation' (25 July 2025) <<https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>>.

2.3.3. Can Automation Enhance the Efficiency of Computational Propaganda?

Computational propaganda promises to shape electoral results by delivering victories or reverse engineering defeats. It aims to shape electoral results, either by facilitating victories or by reverse-engineering defeats to understand what is required to win the campaign. Among the key tools employed in political campaigns are political bots.³⁶⁰ Like other bots, political bots gather, process and analyse data from open-access sources through scraping. In doing so, they intensify the achievement of computational propaganda by targeting voters and facilitate its coordination by automated features. Their automated capabilities allow them to spread faster and more widely, optimizing campaign management.

Tufekci explains computational propaganda as “the campaigns know a lot about individual voters while voters don’t know what campaigns know about them.”³⁶¹ Because computational propaganda turns political communication into an increasingly personalized, private transaction. Wolley and Howard address this concept as a novel propaganda created or disseminated by computational means.³⁶² Accordingly, this propaganda refers to the assemblage of social media platforms, autonomous agents, algorithms, and big data systems that operate to manipulate public opinion.³⁶³ Computational propaganda generally comprises at least one of the following elements: “bots that automate content delivery; fake social media accounts that require some (limited) human curation; and junk news— that is, misinformation about politics and public life.”³⁶⁴ Consequently, computational propaganda-driven strategies capitalize on power asymmetries between individual voters and data brokers, or political bots.

³⁶⁰ Persily and Tucker (n 110) 95.

³⁶¹ Tufekci (n 56) 4. Also see ‘Data Brokers A Call for Transparency and Accountability’ (Federal Trade Commission 2014) 38 <<https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>>.

³⁶² Woolley and Howard (n 53) 5.

³⁶³ *ibid.*

³⁶⁴ *ibid.* However, human curation may no longer be limited.

Moreover, they can violate the fundamental principles and rights regarding political elections, such as right to free elections, democratic elections, unequal media coverage of the electoral campaign. Indeed, as Moore highlights, “this information asymmetry, which enables campaigns to predict voters’ political preferences and attitudes, jeopardises the principle of voter privacy.”³⁶⁵

An election campaign needs two key elements to achieve on digital platforms: first, knowing its target audience and producing content for the audience; second, having enough visibility to reach that audience. This aligns with the platforms’ business model, which provides two interconnected networks: content and advertising. When these models are automated, content can be produced and distributed more rapidly, extensively, and visibly, strengthening the campaign’s impact. Platforms also serve as the infrastructure through which computational propaganda is conducted and, like any digital infrastructure, provide automation opportunities. In 2019, 37.2% of all internet users were robots.³⁶⁶ In 2023, 49.6% of all internet traffic was not human.³⁶⁷ Approximately 48 million Twitter accounts were managed by automated programs in 2020.³⁶⁸ At the beginning, Twitter followed only one precaution against the automation which was Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA),³⁶⁹ however, there was no inspection to detect automated accounts and posts.³⁷⁰ Currently, there are many automation tools and services for conducting campaigns via WhatsApp by pre-defined messages or AI-generated responses. Automated flow for

³⁶⁵ Moore (n 58) 95.

³⁶⁶ Thales Company, ‘Bad Bot Report’ (imperva 2020) 12 <<https://www.imperva.com/resources/resource-library/reports/2020-bad-bot-report/>>.

³⁶⁷ Thales Company, ‘Bad Bot Report’ (imperva 2024) 6 <<https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/>>.

³⁶⁸ Rodríguez-Ruiz and others (n 112).

³⁶⁹ This can be described as an ‘anti-Turing’ test. In the original Turing test, machines seek to persuade human judges of their humanity; here, the situation is inverted, with humans required to prove their humanity to a machine.

³⁷⁰ Zi Chu and others, ‘Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?’ (2012) 9 IEEE Transactions on Dependable and Secure Computing 811, 2 <<https://doi.org/10.1109/TDSC.2012.75>>.

Telegram bots in campaign use is also common. Thus, political bots also utilise this automation in election processes to generate content, rapidly disseminate it, and reach the targeted audience.

As a result, automated bots have become more prevalent,³⁷¹ but they have simultaneously posed a challenge: the question of how to detect them. In some research, different classification is used to understand how it is possible to evaluate if a Twitter account is controlled by human or machine such as network, user, friends, content, sentiment, temporal.³⁷² To detect automated systems, such as humans, bots, bot-assisted humans and human-assisted bots, users on platforms are grouped in categories and used indicators or patterns for analysing them.³⁷³ As bots become more advanced, researchers are exploring new methods, criteria or alternative indicators for their detection.³⁷⁴

³⁷¹ However, research on Finnish Parliamentary elections in 2019 shows that there are regional differences in the prevalence of bot accounts from Germany to Russia and Finland. Another study, focusing on the 2019 elections in Spain, illustrates the growing trend of social bot participation in recent political and administrative elections. The related graph (Figure 1 in the study) shows how this trend has expanded over time, incorporating many additional countries. See details Sippo Rossi and others, 'Detecting Political Bots on Twitter during the 2019 Finnish Parliamentary Election' (2020) 2433 <<https://doi.org/10.24251/HICSS.2020.298>> accessed 19 October 2025; Javier Pastor-Galindo and others, 'Spotting Political Social Bots in Twitter: A Use Case of the 2019 Spanish General Election' (2020) 17 IEEE Transactions on Network and Service Management 2156, 2157 <<https://doi.org/10.1109/TNSM.2020.3031573>>.

³⁷² Clayton A Davis and others, 'BotOrNot: A System to Evaluate Social Bots' <<https://doi.org/10.48550/ARXIV.1602.00975>> accessed 18 August 2023; Emilio Ferrara and others, 'The Rise of Social Bots' (2016) 59 Communications of the ACM 96, 99 <<https://doi.org/10.1145/2818717>>; Maryam Heidari, James H Jr Jones and Ozlem Uzuner, 'Online User Profiling to Detect Social Bots on Twitter' (arXiv, 2022) <<https://doi.org/10.48550/ARXIV.2203.05966>> accessed 2 March 2025; Shao and others (n 19) 9.

³⁷³ Subrahmanian et al. emphasise that bot identification is achieved through a semi-automated process relying on four primary methods: inconsistency detection and behavioural modelling, text analysis, network analysis, and machine learning. See VS Subrahmanian and others, 'The DARPA Twitter Bot Challenge' <<https://doi.org/10.48550/ARXIV.1601.05140>> accessed 19 October 2025; Chu and others (n 370).

³⁷⁴ Zhixiong Chen and Deming Chen, 'Identifying the Invisible: A Comprehensive Approach to Distinguishing Software Bots' (2024); Adrian Rauchfleisch and Jonas Kaiser, 'The False Positive Problem of Automatic Bot Detection in Social Science Research' (2020) 15 PLOS ONE e0241045 <<https://doi.org/10.1371/journal.pone.0241045>>; Doshi and others (n 32).

2.4. Governance of Political Bots Around Elections

Governance of political bots involves multiple actors, including lawmakers, NGOs, public authorities (such as electoral commissions, data protection agencies, and media regulatory bodies), media actors (particularly platforms), and political parties. These actors may adopt varying approaches to political bots, such as platforms' regularly updated terms and conditions, the EU's intricate legislative framework, and the sophisticated technologies employed by political parties. Also, coordination within the limited timeframe of an election is a significant challenge, given its highly demanding and intense nature. As a result, the multiple actors would consider AI systems, thereby AI-driven bots, for governance of political bots.

Governance is defined as an ability to make and enforce rules.³⁷⁵ It can be understood as both top-down and bottom-up, existing both inside and outside organisations.³⁷⁶ As a concept, governance excludes all forms of social ordering which are purely occasional and do not rely on any form of rule, but does not exclude the coordination between actors based on rules.³⁷⁷ Thus, governance manifests itself through principles, rules, and conditions that function as constitutional instruments arising outside the state-centric paradigm.³⁷⁸

³⁷⁵ However, this concept is used as a policy term emerged in Western Europe and North America. Although governance points out specific meanings in cognate disciplines, in general, governance is used to analyse multimodal regulations on multiple levels such as local, regional, or global across multiple dimensions. See Robert Gorwa, 'What Is Platform Governance?' (2019) 22 *Information, Communication & Society* 854, 856; Also see Aphra Kerr, Stefano De Paoli and Max Keatinge, 'Surveillant Assemblages of Governance in Massively Multiplayer Online Games: A Comparative Analysis' (2014) 12 *Surveillance & Society* 320.

³⁷⁶ Jo Pierson, Aphra Kerr and Rob Heyman, 'Meeting Societal Expectations: Cooperative Responsibility in the Design and Governance of AI' (2020) <<https://researchportal.vub.be/en/publications/meeting-societal-expectations-cooperative-responsibility-in-the-d>>.

³⁷⁷ Christian Katzenbach and Lena Ulbricht, 'Algorithmic Governance' (2019) 8 *Internet Policy Review* 2 <<https://doi.org/10.14763/2019.4.1424>> accessed 20 September 2023.

³⁷⁸ Celeste and others conceptualise governance along micro and macro dimensions: while the rules on platforms set for users constitute micro-governance, the regulatory obligations imposed on platforms are classified as macro-governance. Celeste and others (n 245) 13 and 15.

Accordingly, platforms define user rights and govern participation in digital environment at their own discretion. As these rules establish the conditions for participation, they may be viewed as a form of constitutionalism.³⁷⁹ However, this can be regarded as performing an incomplete constitutional function because of the absence of users' representation and their consensus on the terms and conditions of platforms.

Indeed, the platforms take advantage of “remarkable absence of obligations”³⁸⁰ in this well-known digital environment. Thus, platforms have been subject to extraordinary profits. On the other hand, this very lack of regulation has made the governance of bots a pressing issue, especially with the rise in popularity of tools like ChatGPT, keeping the topic at the forefront of policy discussions and legislative agendas such as the AI Act. Due to these legal gaps or regulatory loopholes, platforms have exercised oligopolistic control over most digital information and communication infrastructures, systems, and processes.³⁸¹

They have remained untouchable because of their lobbying activities.³⁸² As long as they keep this untouchable situation, negotiating the rules becomes increasingly difficult.³⁸³ Despite their

³⁷⁹ The terms of service of social media platforms can only be seen as a self-regulatory instrument wielded by a dominant actor within the social media environment. See Edoardo Celeste, ‘Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?’ (2019) 33 *International Review of Law, Computers & Technology* 122, 127 <<https://doi.org/10.1080/13600869.2018.1475898>>.

³⁸⁰ Tarleton Gillespie, ‘The Politics of “Platforms”’ (2010) 12 *New Media & Society* 347, 348 <<https://doi.org/10.1177/1461444809342738>>; Christian Katzenbach and others, ‘Policing Platforms: Addressing Power and Inequalities in Platform Policies’ [2023] *AoIR Selected Papers of Internet Research* 2 <<https://doi.org/10.5210/spir.v2022i0.12959>> accessed 21 July 2025.

³⁸¹ Zuboff (n 252).

³⁸² Niamh Kirk, ‘Lobbying and the Online Influence Industry – Reactionary Regulation of Data Driven Political Campaigns’ (*publicpolicy.ie*, 10 January 2023) <<https://publicpolicy.ie/governance/lobbying-and-the-online-influence-industry-reactionary-regulation-of-data-driven-political-campaigns/>>; Davies (n 61).

³⁸³ An example can be from Turkey. In January 2020, in response to the 93 million Turkish Lira fine imposed by the Turkish Competition Authority, Alphabet not only declared that it would not comply with this sanction but also suspended access to its services, such as Google Maps, in Turkey for several days. This example shows that their positions are based on fundamentally non-negotiable grounds.

See Gizem Yardımcı and Altug Yalcintas, ‘The Issue of Central Planning in Big Data Age (Büyük Veri Çağında Merkezi Planlama Meselesi: Dijital Korumacılık mı, Sansür mü?)’ *Özne | Volume 33: Science and Society Studies*, vol 33 (Çizgi Kitabevi 2021).

supposed neutrality and transparency, platforms have released detailed policies and conditions on who can say what and where.³⁸⁴ Therefore, understanding the role and position of platforms within power relations is also essential for grasping the utility of political bots. This understanding helps to recognise the importance of regulating political bots particularly in light of the business model in which they operate.³⁸⁵ Once the utility of political bots is understood, the importance of regulating them becomes clearer, particularly in light of the business model within which they operate.

Using political bots is a clear advantage for political campaigners. The more a candidate or campaign is amplified, or the more effectively they discredit their opponents, the more visible and popular they become. Even the algorithms often reinforce this dynamic by prioritising such content shared by candidates or their teams. Political bots also serve the interests of states, as they can, at times, contribute to the formation of political public opinion. For the platforms, the use of political bots is beneficial as well, since user attention remains locked on the platform. Contrast to common theories or assumptions, the relationship between governments and Big Tech companies that own the platforms may not be one of power asymmetry, but rather one of power alignment.

For this purpose, political campaigns employ populist narratives. According to Sjöström, public opinion is still formed by the interaction and, also traditional media still frames the

³⁸⁴ Another example is the case of Platform X, which, as of 19 March 2025, deleted or suspended numerous user accounts in Turkey that produced and disseminated content critical of the government. These posts formed part of the protests that intensified in response to the arrest of Istanbul Mayor Ekrem İmamoğlu. See From Platform X Global Government Affairs, 'Global Government Affairs' (23 March 2025) <<https://x.com/GlobalAffairs/status/1903879657755230507?s=20>>.

³⁸⁵ Platform services are designed to benefit from advertising-driven business model. This kind of service may cause concerns in society. As this article also highlights, in the absence of effective regulation and enforcement, platforms may set the rules for the game, which, indeed, they have done. See more Noémi Bontridder and Yves Poulet, 'The Role of Artificial Intelligence in Disinformation' (2021) 3 Data & Policy 16 <<https://doi.org/10.1017/dap.2021.20>> accessed 21 July 2025.

picture.³⁸⁶ Indeed, social media and traditional media feed each other, amplifying entertaining debate. However, one dynamic shared by these two media spheres is the use of political bots to advance populist goals.

Another emerging dynamic is the dissemination of deepfake-embedded content. For instance, during the 2023 Turkish Presidential elections, a deepfake video of the opposition leader was spread by the Ak Party candidate and President Recep Tayyip Erdogan, just three days before the election and was not taken down.³⁸⁷ Even if the removal of such content were to be requested through the courts or an appeal was made to the Supreme Election Council, in an autocratic regime that has seized control of all institutions over its 21-year rule, it is unrealistic to expect the process to be conducted swiftly and in a way that prevents rights violations. Indeed, this did not happen. Platforms could not restrict the content on time, while traditional broadcast media, already under the influence of the ruling party, Ak Party, continued to disseminate the footage. During the same period, platform algorithms promoted false news concerning candidates among their top content recommendations.³⁸⁸ In this case, the responsibility cannot fall solely on the platforms.

³⁸⁶ Torbjörn Sjöström, 'The Rise of Populism – A Presentation by Torbjörn Sjöström, from Novus and Gallup Nordic.' (WAPOR 78th Annual Conference, St. Louis, Missouri, USA, 12 May 2025) <<https://youtu.be/bzjNIIPZGzk?si=nHtKZ5WN6HKF0YGX>>.

³⁸⁷ Pelin Ünker and Thomas Sparrow and May 24, 2023, 'Fact Check: Turkey's Erdogan Shows False Kilicdaroglu Video' *Deutsche Welle* <<https://www.dw.com/en/fact-check-turkeys-erdogan-shows-false-kilicdaroglu-video/a-65554034>>; Jana Schaich Borg, Walter Sinnott-Armstrong and Vincent Conitzer, *Moral AI: And How We Get There* (Pelican, an imprint of Penguin Books 2024) 17.

³⁸⁸ Turkey is referred to frequently throughout this study for three main reasons. First, Turkey was politically highly polarised during the 2023 general elections, a situation that was also reflected in voter turnout. Second, after the 2013 Gezi Park protests, increasingly strict and systematic measures were adopted against forms of public mobilisation organised through digital technologies. These measures, including broader developments in technology governance and AI-related regulatory approaches, have also had implications for electoral processes. Third, despite not being an EU member state, Turkey represents one of the countries where relatively early and experimental forms of digital technologies in electoral processes have been observed. As a result, Turkey provides an important, timely and novel example for examining the relationship between digital political communication, governance, and democratic processes. Samantha Bradshaw and Philip N Howard, 'Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation' (Computational Propaganda Research Project of Oxford University) 3 and 22.

The accountable actors must include not only the platforms but also the legal mechanisms that should have been promptly activated, along with all democratic institutions and mechanisms of the country. Therefore, political parties, higher judicial bodies, and platforms must work together. For this reason, in addition to platforms, political parties, candidates, public authorities such as the Electoral Commission in Ireland (*An Coimisiún Toghcháin*), and the Supreme Election Council in Turkey (*Yüksek Seçim Kurulu*), are responsible for regulating, managing, and overseeing electoral processes, and the actors involved in a political movement or strategic political alliances are also expected to be held accountable. In accordance with accountability, transparency, and trustworthiness, these actors are expected to be responsible also for ensuring the accuracy of the information being disseminated, and auditing the content of shared materials on digital platforms. This is a structural prerequisite for democratic institutions. As a result, the responsible election commissions appear to be unprepared for digital manipulation tools.

In both traditional and social media, emotions tend to trump knowledge. This tendency makes content that exploits emotions more likely to become popular.³⁸⁹ In both media sectors, this manifests as entertaining debates, which also guarantee profits for media organisations. This tendency makes content that exploits emotions more likely to become popular. The media outlets, in traditional or digital, guarantee profits via entertaining debates for each topic. This form of debate can create a false balance, where facts are replaced by ‘alternative facts’. As a result, uncertainty grows, and people begin to question who or what they can trust. This cycle operates in both media sectors.

³⁸⁹ Dickerson, Kagan and Subrahmanian (n 155).

Rather than addressing real solutions, the electoral strategies that serve populism encourage an ‘emergency break’ during crises invented by the political environment. For the same reason, while traditional political parties tend to focus on developing solutions, strategies, or long-term plans in case they gain power, newer political parties may rely more on populist narratives. Faced with weak or unsupported policies, citizens may ultimately turn to populist parties or leaders as a perceived emergency solution.

Therefore, political bots, as the most suitable digital tools for spreading populist narratives, may be adopted by all political actors. At the same time, political bots also serve the interests of states, as they can, at times, contribute to the formation of political public opinion. For the platforms, the use of political bots is beneficial as well, since user attention remains locked on the platform.

In contrast to common theories or assumptions, the relationship between governments and Big Tech companies that own the platforms may not be one of power asymmetry, but rather one of power alignment. However, the recent updates from the platforms show that when this power relationship does not serve the interests of Big Tech companies, platforms tend to seek alternative routes to avoid complying with regulations. The most recent example of this is Google³⁹⁰ and Meta announcing,³⁹¹ from early October 2025, that they would not meet the requirements of the TTPA.³⁹²

³⁹⁰ Annette Kroeber-Riel, ‘An Update on Political Advertising in the European Union’ (14 November 2024) <<https://blog.google/around-the-globe/google-europe/political-advertising-in-eu/>>.

³⁹¹ META, Newsroom for Europe, Middle East and Africa (n 359).

³⁹² Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (n 41).

Meta, in particular, justified its decision by claiming that the TTPA creates an ‘untenable level of complexity and legal uncertainty’ for advertisers and platforms within the EU.³⁹³ Google also mentions that broad definition of political advertising is one of the reason.³⁹⁴ Specifically, Meta announced that, in the EU only, it would stop offering the service of publishing paid political advertisements on its platforms.³⁹⁵ Both Meta and Google cited regulatory challenges as the reason for their decisions.³⁹⁶ However, it is clear that even when regulations involve legal uncertainties or operational challenges, platforms have been complied with the EU legislative framework. In the case of this regulation, in TTPA, withdrawal of paid advertising services from the EU, thereby remaining outside of regulation, reflects dissatisfaction of these companies with the legal framework. Whether this approach will remain limited to the TTPA is currently unknown. In particular, the withdrawal of services in response to challenges posed by any regulation could, over time, become another strategy within this power dynamic.

In addition, Meta has emphasised that its decision will not prevent people in the EU from continuing to discuss politics on its platforms, nor will it stop politicians, candidates, and political officials from organically producing and sharing political content.³⁹⁷ Google has also stated that it will ensure voters have access to high-quality and reliable information.³⁹⁸ Nevertheless, the risks posed by political bots in electoral processes are likely to increase in any case.

This is because political bots will increasingly serve as an alternative to paid advertisements, and while their AI-driven nature will enable them to produce content faster and in greater

³⁹³ META, Newsroom for Europe, Middle East and Africa (n 359).

³⁹⁴ Annette Kroeber-Riel (n 390).

³⁹⁵ META, Newsroom for Europe, Middle East and Africa (n 359).

³⁹⁶ Annette Kroeber-Riel (n 390); META, Newsroom for Europe, Middle East and Africa (n 359).

³⁹⁷ META, Newsroom for Europe, Middle East and Africa (n 359).

³⁹⁸ Annette Kroeber-Riel (n 390).

volume, the real problem lies in the fact that the programs behind these bots will not have legal personhood. Another concern is that the numerous exemptions the AI Act regulates for AI systems used in democratic processes will leave a legal gap, making democratic processes vulnerable to political advertising through bots.

As noted above, within this mutual benefit structure, the claim that platforms genuinely struggle to detect bots appears less convincing in light of existing research.³⁹⁹ This is because technological developments do not solely favour the proliferation and undetectability of bots. Surprisingly, new methods for identifying bots have also emerged via advanced AI tools.⁴⁰⁰ In fact, bots can be detected even through studies based solely on data provided by Platform X.

Moreover, platforms may develop detailed content policies about user activities, and often aligned with state interests.⁴⁰¹ These arrangements are frequently based on negotiations with member states that bypass citizens. Instead of a power asymmetry, there may be a power alignment. This is especially evident when platforms engage in implicit or explicit alignments with political actors or parties that are likely to win elections. Moreover, their future interest in maintaining favourable relations and visibility during electoral processes.⁴⁰²

At the core of all these power symmetries or asymmetries, users remain as a passive actor. Despite being a prosumer,⁴⁰³ both producing and consuming content, users are excluded from every other aspect of the process. Political bots are artificial user groups that, at times, benefit from this power relationship. Although political bots have no say in matters of governance

³⁹⁹ MHM Schellekens, 'Are Internet Robots Adequately Regulated?' (2013) 29 Computer Law & Security Review 666, 666 <<https://doi.org/10.1016/j.clsr.2013.09.003>>.

⁴⁰⁰ Ferrara, 'Social Bot Detection in the Age of ChatGPT' (n 153).

⁴⁰¹ Moore and Tambini (n 342) 198.

⁴⁰² Karen Weise and Maggie Haberman (n 48).

⁴⁰³ Toffler (n 246) 265–282; Kasap and Yalcintas (n 246).

directly, their activities are often overlooked by platforms for specific reasons. First, due to the fast-paced nature of electoral processes, specifically the short period between campaigns and voting day, even if the disruptive and manipulative interventions of political bots are brought before the judiciary, court decisions are often announced after the elections, resulting in delayed justice. Second, platforms may adopt a flexible approach to political bot activity and choose to ignore such actions. As a result, the governance of political bots encompasses all parties that establish, release, implement, and monitor the rules governing their function, including the platforms themselves. However, there is no room for negotiation in the platforms' approach to the governance of bots. Additionally, the democratic deficit in AI governance⁴⁰⁴ leads to the proliferation of political bots.

Any governance initiative that lacks negotiation is, by nature, anti-democratic. As Celeste and others highlight, social media companies hold the power to unilaterally formulate and modify their terms of service without any requirement for transparency or democratic legitimacy, resembling an "absolutist" regime.⁴⁰⁵ Accordingly, in the digital sphere, the formulation, articulation, and implementation of principles that, in the analogue world, would be enshrined in constitutions, now rest solely in the hands of a single decision-maker: the social media company.⁴⁰⁶

Thus, users can access platforms only if they accept the terms and conditions set by these platform regimes. When the terms and conditions are updated, the user has no choice but to accept them; otherwise, users may not access their account. This is closely linked to widespread

⁴⁰⁴ Johannes Himmelreich, 'Against "Democratizing AI"' [2022] AI & SOCIETY 1337 <<https://doi.org/10.1007/s00146-021-01357-z>> accessed 14 November 2022.

⁴⁰⁵ Celeste and others (n 133) 13; Johannes Himmelreich, 'Against "Democratizing AI"' [2022] AI & SOCIETY 1337 <<https://link.springer.com/10.1007/s00146-021-01357-z>> accessed 14 November 2022.

⁴⁰⁶ *ibid* 14.

use of political bots in election processes. Accounts with high interaction with bot activities may be suspended or can be eliminated through effective detection mechanisms by platforms. Moreover, platforms not only have the power to implement their self-regulations but also the authority to judge cases based on their terms and conditions or community standards. According to Meta, it was necessary to establish the Oversight Board when the Facebook community reached out to 2 million people.⁴⁰⁷ Then, the Board started to discuss and formalise desired operating procedures and hear the first case in 2020. Since February 2024, the Board expands its scope to include Threads as well as Facebook and Instagram. The board released governing documents on their web page such as its trust agreement, limited liability agreement of Oversight Board LLC, charter, bylaws, rulebook, overarching criteria.

However, the Board gained popularity in 2021 following its ruling on President Trump's case.⁴⁰⁸ The assessment of the facts and the reaction of Facebook could cause another violence or violence threatened the constitutional process.⁴⁰⁹ At the end of the analysis, the Board released a policy advisory statement. According to the statement, regular processes of Facebook would not prevent or avoid imminent harm during crises or novel situations. The Oversight Board continues to decide on implementation of community standards. Similarly, preventive measure implemented by platforms against bots engaged in disinformation, deepfake dissemination, or manipulative activities must be precisely define to avoid censorship.

⁴⁰⁷ 'The Oversight Board' (<https://www.oversightboard.com/>).

⁴⁰⁸ Ivana Vukčević, 'Facebook Oversight Board's Decision on the Indefinite Suspension of Donald Trump's Account' (2021) 12 *Pravni zapisi* 295 <<https://doi.org/10.5937/pravzap0-32521>>.

⁴⁰⁹ Former President Trump's suspension [2021] The Oversight Board case 2021-001-FB-FBR.

Apart from these, in some countries such as Turkey,⁴¹⁰ governments may require social media accounts be linked to national ID numbers or ID Cards for bot and trolls detection.⁴¹¹ Before elections, governments may issue non-transparent directives to platforms regarding algorithm management, disinformation control, and content moderation.⁴¹² When the platforms fail to comply with demands, governments may take technical actions such as threat to throttle the service.⁴¹³ Platforms, in turn, may object to the court orders, and share the regulators' correspondence to ensure the transparency instead of the government.⁴¹⁴ This highlights the clear power asymmetry between states and platforms, as government could take a more prohibitive position.⁴¹⁵ Nonetheless, users remain the ones most affected by the policies and enforcement actions of both actors.⁴¹⁶

Second, public authorities, as in the case of the AI Act, may formally invite public input during regulatory processes. However, limited access to the internet, devices, or digital literacy may prevent individuals from sharing their perspectives. Furthermore, the Artificial Intelligence High Level Expert group (AI-HLEG)⁴¹⁷ was comprised of experts from the humanities, social

⁴¹⁰ Also, please see Section 2.2.2, "Are Political Bots the Digital Continuation of Traditional Media in Electoral Campaigns?", for a more detailed explanation of the inclusion of examples from Turkey.

⁴¹¹ 'The Grand National Assembly of Turkey Minutes Magazine (Türkiye Büyük Millet Meclisi Tutanak Dergisi)' 450.

⁴¹² 'Global Government Affairs' <<https://x.com/GlobalAffairs/status/1658208072215437314>>.

⁴¹³ *ibid.*

⁴¹⁴ *ibid.*

⁴¹⁵ From the AI and democracy perspective, Risse highlights that AI and democracy are not "natural allies". This is because ensuring that AI serves democratic purposes requires "active design choices" and strong political will. Mathias Risse, 'Artificial Intelligence and the Past, Present, and Future of Democracy' in Silja Voienky and others (eds), *The Cambridge Handbook of Responsible Artificial Intelligence* (1st edn, Cambridge University Press 2022) <<https://doi.org/10.1017/9781009207898.009>> accessed 20 October 2025.

⁴¹⁶ This research asks who the new information fiduciaries are in the digital age. It reflects that organisations and enterprises that collect enormous amounts of data enjoy significant asymmetries of knowledge and power over their end-users. Jack M Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2017] SSRN Electronic Journal 14 <<https://doi.org/10.2139/ssrn.3038939>> accessed 20 September 2023.

⁴¹⁷ Jo Pierson et al., 'Governing Artificial Intelligence in the Media and Communications Sector' (2023) 12 Internet Policy Review 5 <<https://policyreview.info/articles/governing-artificial-intelligence-media-and-communications-sector>> accessed 21 March 2023.

sciences, and technical domains.⁴¹⁸ However, some fields, such as computer science and engineering, appeared to be more prominently represented, raising concerns about whether all disciplines were equally represented in providing public input on potential AI regulation. This expert group published the White Paper⁴¹⁹ advising on the AI Act.⁴²⁰ As a consequence, it appears that even in the professional framework recommending AI regulation, there exists a democratic representation gap across all scientific disciplines in the governance of AI systems.

On the other hand, political parties declare their ethical principles in their party programs. They promise to conduct their political activities, including campaigns, in align with national legal regulations.⁴²¹ Thus, political parties remain subject to AI governance policies established by governments. NGOs, in contrast, engage in EU regulatory processes by submitting opinions, shaping AI governance and policies on political bots. Consequently, the power of actors beyond platforms and governments in shaping AI governance remains limited.

2.5. Conclusion

Bots have evolved from simple rule-based programs to advanced AI-driven models. They have transformed digital interactions, including political communication. As Habermas emphasises, the public sphere is becoming increasingly fragmented, and the boundaries between different spheres are dissolving. This challenges the democratic role of political discourse, especially

⁴¹⁸ The working group consisted of 52 members. There were no academics from media and communication studies, from traditional public service media or new digitally native European media companies. See Gizem Yardımcı, Aphra Kerr and David Mangan, 'The Social Science Deficit in AI Regulation: An Analysis of the Composition of the European Commission's High-Level Group of Experts on Artificial Intelligence and Implications for Technology Regulation.' (2023 conferences of the International Association for Media and Communication Research (IAMCR), Lyon, 9 July 2023) <<https://iamcr.org/node/30133>>.

⁴¹⁹ European Commission. Directorate General for Communications Networks, Content and Technology., 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust' (2020) COM(2020) 65 final.

⁴²⁰ Artificial Intelligence Act (n 40).

⁴²¹ Herri Batasuna and Batasuna v Spain Application No 25803/04 and 25817/04 (European Court of Human Rights).

with the rise of political bots influencing electoral processes. The new power asymmetries between states, platforms, and political actors complicate accountability and regulatory oversight. The differences and complexity in the governance of AI-driven political communication, particularly political bots, demonstrate the irregularities in power asymmetries and the lack of coordination among actors.

This chapter applied Habermas's public sphere theory to political bots and developed the theoretical framework of this thesis. In the next chapter, Chapter 3, it examines the legal framework of political bots within the context of EU law. In particular, the activities of political bots are assessed in relation to the Charter of Fundamental Rights of the European Union, the AI Act, and the Digital Services Act. In this way, the theoretical framework developed in Chapter 2 is connected with the legal framework discussed in Chapter 3.

Chapter 3: Legal Framework in the AI Act for Political Bots

3.1. Introduction

This chapter outlines the legal framework of political bots with a particular focus on the EU legislation. As the research question of this thesis asks how the AI Act could prevent using political bots as manipulative tools during political elections, this chapter investigates how political bots are regulated in the EU by analysing recent EU legislation, namely the AI Act. The analysis advances a response to the thesis's research question: How might the AI Act prevent the use of political bots as manipulative tools during political elections?

The chapter presents an assessment within the framework of rights and freedoms. This chapter aims to provide legal and doctrinal findings. It proceeds in two main steps. First, the chapter explores how political bots are regulated under the AI Act. This assessment follows a structured approach: it begins by questioning whether the objective and scope of the AI Act meaningfully overlap with the functions of political bots. Then, it analyses which types of political bots fall within the definition of AI systems. It moves on to address how political bots might be categorised under the AI Act's risk-based approach, especially whether they could be considered high-risk systems. If political bots are recognised as high-risk AI systems, this analysis focuses on, if necessary, how the requirement to conduct a fundamental rights impact assessment (FRIA) would apply to them. In addition, the chapter considers the legal framework of the AI Act for generative-AI driven political bots. This is because the advanced political bots are supported by generative-AI characteristics. Thus, the first part of this chapter explores to what extent the AI Act is capable of protecting democratic processes against the potential manipulative strategies posed by political bots.

Second, the chapter investigates whether political bots can enjoy freedom of expression and information as enshrined in the CFR. This section proceeds by critically assessing whether accuracy matters for freedom of expression and information. Additionally, the section focuses on whether the political bots must provide accurate information, or users must reach out for the accurate information on platforms and what the responsibilities of political bots and platforms are. It also questions whether freedom of expression and information is relevant to, or could be extended to cover, the actions of non-human actors such as robots and bots. Finally, it discusses whether political bots can be considered as a subject of freedom of expression and information within the CFR, and whether their communicative functions would fall under a framework of rights limitations or prohibitions.

3.2. How Does the AI Act Regulate Political Bots?

The AI Act is an attempt to regulate AI systems in the EU, and constitutes the first comprehensive legal framework in this domain. While it is often described as the first legal regulation of AI, this is only partially accurate: the Council of Europe had already issued relevant documents before the AI Act became official.⁴²² The regulation has faced various criticisms, including being overly complex, heavily influenced by lobbying, rushed in an attempt to be the first of its kind, or, conversely, delayed in responding to the rapid development of AI systems. Despite these critiques, the legislative process endured, incorporated many of the concerns raised, and ultimately resulted in one of the EU's most recent legal instruments.

⁴²² According to the Council of Europe, this document is the “first-ever internationally binding treaty” regarding in the AI field. It aims to ensure activities of AI systems lifecycle align with human rights, democracy and rule of law. Also, the document aims to fill the legal gaps in case it relies on rapid tech advances. However, it was adopted on 17 May 2024 by the Committee of Ministers of the Council of Europe at its 133rd Session held in Strasbourg, then it was opened for signature on the occasion of the Conference of Ministers of Justice in Vilnius (Lithuania) on 5 September 2024. See Committee on Artificial Intelligence (CAI), Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law 2024 [CM(2024)52-final]; The Council of Europe, ‘The Framework Convention on Artificial Intelligence’ (*The Council of Europe*) <<https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>>.

The regulation entered into force on 1 August 2024. The majority of rules will begin applying on 2 August 2026. For the content of this thesis, definitions and provisions related to AI literacy became applicable 6 months after the entered into force on 2 August 2025. Also, the obligations for high-risk AI systems, which are directly relevant to the content of this thesis, will apply 36 months after their entry into force on 2 August 2027.

The Act regulates political bots, as they are currently AI-enabled bots. However, whether the Act adequately addresses the specific risks and harms these bots may generate remains questionable. There may be two main reasons for this.

First, there is no clarity on why this product-based regulation ended up touching democratic processes while regulating AI systems. This structure of regulation becomes the clearest sign that democratic processes are treated as a business field. AI Act approaches AI systems primarily as products and applies to businesses that create or use AI systems, alongside other actors. This product-based approach was quite clear from the beginning, particularly during the 2022 discussions on new liability rules for AI and products in the draft AI Act, framed both to foster innovation and to protect consumers. As one of the interviewees analysed in Chapter 4 highlighted, the product-based approach of the Act clearly limits expectations concerning fundamental rights (SG2-Interview 4, Pos. 39).

The AI Act conceptualises these systems and focuses on deployers and providers. Even when these systems are used in democratic processes, the focus remains on the providers and deployers. The AI Act does not directly regulate fundamental rights, particularly through the choice of terminology, appears to have increased interpretative uncertainty. As a result, when

these systems interfere with fundamental rights and freedoms, the regulatory response tends to prioritise market conformity over rights protection.

Second, the regulation of the AI market and business environment has allowed big tech companies, alongside EU citizens, to become active participants in the regulatory process. This, in turn, has raised concern about a blurring of the boundaries that the regulation draws around the protection of fundamental rights and freedoms. This legal assessment outlines the dimensions through which political bots are regulated under the AI Act. The following section seeks to illustrate how the two initial arguments -these main reasons- are embedded in the design and implementation of the legal framework for political bots. Thus, it explores the specific regulatory dimensions applicable to political bots under the AI Act, including their classification as high-risk systems, their relation to chatbots and GPAI, and transparency-related obligations.

3.2.1. Are Political Bots Within the Scope of the AI Act?

To determine whether political bots constitute AI systems that fall within the scope of the AI Act requires examining Article 2, which explains the scope of the AI Act, and Article 3, which establishes the definition of AI systems. According to Article 2 of the AI Act, there are specific points which explain certain areas of the Regulation. An assessment of the scope and definition of AI systems from the perspective of political bots is set out below.

Political bots were initially designed as simple digital tools that mimicked human behaviour.⁴²³

They were embedded on social media platforms such as Twitter, Telegram, or Reddit.⁴²⁴ They

⁴²³ Ferrara, 'Social Bot Detection in the Age of ChatGPT' (n 153) 7.

⁴²⁴ VAH Firdaus, PY Saputra and D Suprianto, 'Intelligence Chatbot for Indonesian Law on Electronic Information and Transaction' (2020) 830 IOP Conference Series: Materials Science and Engineering 022089, 2 <<https://doi.org/10.1088/1757-899X/830/2/022089>>; Zi Chu and others, 'Who Is Tweeting on Twitter: Human,

are machine-based systems that operate with varying levels of autonomy, such as posting messages or engaging in online conversations without human intervention (referred to as tasks). The outputs they generate reflect influence on virtual and physical environments, such as social media platforms. Additionally, political bots can be adaptive, adjusting their behaviour based on the input they receive -whether this input is provided by users or identified through trending topics on social media platforms.

In their early forms, these bots often repeated identical messages, failed to sustain human-like conversations, and primarily interacted with other bots. As a result, they were relatively easy to detect. However, recent developments in technology, particularly advancements on LLMs such as GPT, Gemini and LLaMA, have significantly transformed the nature of chatbots including political bots. As Barberá highlights, LLMs are advanced deep learning models.⁴²⁵ They are designed to process and generate human-like language.

More detailed information on LLMs is provided in the introduction of this thesis.⁴²⁶ Nevertheless, it is important to emphasise that the new generation political bots are based on LLMs because these models are built to produce and interpret language in a way that mimics human communication. This characteristic is also an essential function of political bots. On a deeper level, political bots, like other LLM-based models, generate responses by recognising

Bot, or Cyborg?’ *Proceedings of the 26th Annual Computer Security Applications Conference* (ACM 2010) 21 <<https://doi.org/10.1145/1920261.1920265>> accessed 28 August 2023; Rachel Leingang, ‘X’s AI Chatbot Spread Voter Misinformation – and Election Officials Fought Back’ (12 September 2024) <<https://www.theguardian.com/us-news/2024/sep/12/twitter-ai-bot-grok-election-misinformation>>; Kiel Long and others, “‘Could You Define That in Bot Terms’?: Requesting, Creating and Using Bots on Reddit’ *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (ACM 2017) <<https://doi.org/10.1145/3025453.3025830>> accessed 16 July 2025.

⁴²⁵ Isabel Barberá, AI Privacy Risks & Mitigations – Large Language Models (LLMs) (European Data Protection Board 2025) 6 <<https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf>>.

⁴²⁶ See Chapter 1.

patterns and relationships between words, a core capability of these models. Thanks to the advanced versions of these models make political bots considerably harder to detect.⁴²⁷

However, the AI Act does not regulate AI models until they are not integrated into an AI system.⁴²⁸ The Act defines GPAI models as a component of AI systems. AI models require further components, such as user interface, or application layers, to constitute AI systems.⁴²⁹ Thus, new-generation political bots qualify as AI systems that operate on the basis of LLMs, foundational AI models. Indeed, political bots require a platform and a user interface to reach real users and interact with them. However, the term "AI system" refers to a machine-based system designed to function autonomously at various levels.⁴³⁰ It can demonstrate adaptiveness after deployment, using the input it receives to generate outputs—such as predictions, content, recommendations, or decisions—that influence physical or virtual environments, either for explicit or implicit objectives.⁴³¹ Thus, the definition of AI systems covers political bots. Additionally, political bots are not limited to being a standalone model. They include components such as a generative AI model, a platform, and a user interface, therefore, they qualify as an “AI system” under the AI Act. In this research, political bots are examined as AI-driven bots in view of emerging technological trends.

⁴²⁷ Philip N Howard, Samuel Woolley and Ryan Calo, ‘Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration’ (2018) 15 *Journal of Information Technology & Politics* 81, 84 <<https://doi.org/10.1080/19331681.2018.1448735>>; Ferrara, ‘Social Bot Detection in the Age of ChatGPT’ (n 153) 19.

⁴²⁸ See definition of General-Purpose AI Models in Article 3 (63). Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 152).

⁴²⁹ Recital 97 *ibid.*

⁴³⁰ The AI Act adopts both a machine-based and logic-knowledge-based approach. Machine learning refers to AI systems learning from data how to achieve explicit or implicit objectives. Logic-knowledge-based systems, on the other hand, infer from encoded knowledge or symbolic representation of tasks. This means AI systems go beyond basic data processing, namely, they are capable of modelling, learning, and reasoning. See Recital 12 *ibid.*

⁴³¹ *ibid.*

In Article 2 of the AI Act, AI systems, which are outside the scope of the regulation, are listed. Among these exclusions is the use of AI systems for research and development purposes. According to Recital 25, the main reason for this exemption is the protection of the freedom of science. According to Article 2(6), political bots may also be excluded from the scope of the Regulation, if they are used for scientific research and development. For instance, research in 2019 proves that bots make up a large proportion of the Russian political Twittersphere.⁴³² The 2019 research relies on a very large collection of tweets about Russian politics from 2014-2018. In this research, the meta-data is gathered with tweets via Twitter API.⁴³³ In this example, X platform provides large datasets for academic research purposes.⁴³⁴ In another example, research shows how public surveys can be corrupted at scale. It also reveals that how vulnerable polling has become. In this research, a simple AI tool is operated to examine the vulnerability of online surveys regarding public opinion.⁴³⁵

However, the classification framework of the AI Act tends to become blurred or more complex, especially at the points where political bots intersect with GPAI systems. A clear example of this is how the AI Act assess systemic risks for GPAI models, however, it categorizes AI systems considering their risk levels, such as unacceptable risk, high-risk, minimal risk or exempt AI systems. Prior to engaging with the risk categorisation of political bots, a preliminary assessment is required to identify the conditions under which political bots may be

⁴³² Denis Stukal and others, 'The Use of Twitter Bots in Russian Political Communication Online' (PONARS Eurasia Policy Memo 2019) 564 9.

⁴³³ *ibid* 2.

⁴³⁴ X platform provides public X data by using X API to get historical and real-time data for research purposes. Even the platform X provides this opportunity under DSA Article 40, it is necessary to apply for API access tiers. For this purpose the platform also required the filling of a form from the researchers. See form 'Exploring Twitter's API for Academic Research Purposes' (*X Developers*) <<https://devcommunity.x.com/t/exploring-twitter-s-api-for-academic-research-purposes/224809>>; 'X DSA Researcher Application' (*xAI*) <https://docs.google.com/forms/d/e/1FAIpQLSdo0O-D6Kxa3cV4g1JLz2T_0Sk3hdEnTdv8dJmibagCnzJ7kg/viewform>.

⁴³⁵ Sean J Westwood, 'The Potential Existential Threat of Large Language Models to Online Survey Research' (2025) 122 *Proceedings of the National Academy of Sciences* e2518075122, 2 <<https://doi.org/10.1073/pnas.2518075122>>.

excluded from the scope of the AI Act. Accordingly, the most possible scenario in which political bots may be excluded from the scope of the AI Act is their use for research and development purposes, specifically within the field of political science, demographic research, or statistical studies conducted within a social science context.

3.2.2. Risk-based Categorisation of Political Bots Under the AI Act

Bots are low-risk AI systems under the AI Act. However, when used in democratic processes, they are classified as high-risk AI systems.⁴³⁶ By definition,⁴³⁷ any political bot used for political purposes is inseparable from democratic processes. As detailed in Chapter 2, their very function is to influence, shape, or amplify political public opinion during political campaigns. So, political bots are high-risk AI systems under the AI Act. In light of the AI Act's regulatory framework, questioning the classification of political bots as high-risk appears misplaced.

In this section, to effectively address the question of how and in which category the AI Act regulates political bots, it is first necessary to clarify their relationship with chatbots.⁴³⁸ Political bots, similar to chatbots, are also a type of bot,⁴³⁹ and they are conversational agents.⁴⁴⁰ However, they are generally understood as a special case of social bots,⁴⁴¹ typically used for

⁴³⁶ Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 152) Annex III.

⁴³⁷ This definition does not originate from the AI Act itself. Rather, it is based on an analytical interpretation developed through a review of existing academic literature on political bots.

⁴³⁸ For this relationship and for the detailed information about chatbots and political bots see Chapter 1, section 1.1.4. *What are Political Bots?*

⁴³⁹ This is why this research focuses on chatbots which include political bots. See details about social bots Christian Grimme and others, 'Social Bots: Human-Like by Means of Human Control?' (2017) 5 Big Data 279, 280 <<https://doi.org/10.1089/big.2017.0044>>.

⁴⁴⁰ See more about conversational agents, Amalia Diurni and Giovanni Riccio, 'ChatGPT: Challenges and Legal Issues in Advanced Conversational AI' (2023) 9 Italian Law Journal 473; Lessio and Morris (n 75).

⁴⁴¹ Lucille Van Vooren, '(Dis)Information Warfare Why Online Disinformation Is Able to Prosper and How to Fight It' (University of Bologna 2022) 15.

political purposes.⁴⁴² Ultimately, political bots, social bots, and chatbots all fall under the broader category of bots. Therefore, examining how the AI Act regulates chatbots is essential, as it provides a relevant basis to understand the regulatory framework of political bots in the Act. As a result, the Act defines AI systems rather than AI itself.⁴⁴³ Political bots can be defined as AI systems according to this definition. As such, they fall within the scope of the AI Act.

The AI Act classifies AI systems into categories based on their risk levels. Accordingly, unacceptable risk is defined as ‘prohibited AI practices’.⁴⁴⁴ High-risk AI systems⁴⁴⁵ and GPAI models⁴⁴⁶ limited-risk AI systems⁴⁴⁷ are regulated as other categories. Before the widespread release of OpenAI's ChatGPT,⁴⁴⁸ the categorization was different.⁴⁴⁹ However, as the impact of chatbots became apparent,⁴⁵⁰ amendments were made before the enactment of the AI Act, resulting in the regulation of what is known also as generative AI.

Additionally, the emergence of generative AI and its impact on the draft versions of the AI Act served, in many ways, as a stress test for the regulation’s own purpose and integrity. Although the stated goal of the AI Act has always been to promote innovation, the document itself had to adapt its structure in response to innovation, indicating that its original design was not as solid as intended. This structural fragility raises doubts about the Act’s ability to remain valid in the face of future technological developments. As a result, new classifications had to be

⁴⁴² Van Vooren (n 441).

⁴⁴³ Article 3 (1) Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 152).

⁴⁴⁴ Corrigendum to the position of the European Parliament Artificial Intelligence Act 2024 (cor01) Article 5.

⁴⁴⁵ *ibid* Article 6.

⁴⁴⁶ General-purpose AI models are classified as general-purpose AI models with systemic risk if they meet the conditions listed in Article 51. *ibid* Article 51.

⁴⁴⁷ Transparency obligations for providers and deployers ensure that end-users are aware interacting with AI (chatbots and deepfakes). *ibid* Article 50.

⁴⁴⁸ ChatGPT was released on November 30, 2022, by San Francisco-based OpenAI.

⁴⁴⁹ The risk categorisation was prohibited AI systems, high-risk AI systems, limited risks and minimal risks.

⁴⁵⁰ ‘General-Purpose Artificial Intelligence’ (European Parliament March2023)

<[https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA\(2023\)745708_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf)>.

added, such as "systemic risk" and the FRIA. Additionally, Recital 12 introduces the concept of flexibility as a mechanism to allow the regulation to adjust to ongoing and unforeseen developments in the AI landscape.

These recent amendments in this regulation also focused on the risks caused by generative-AI driven bots and their functions. The reason is that the AI Act adopts a risk-based approach. Generative AI and generative AI-driven systems must be categorized in this regulatory structure to fit them into this risk-based framework. In the context of this research, these amendments mentioned above because of the OpenAI's ChatGPT, specifically refer to generative AI chatbots, as they become the common basis of political bots in this era.

While bots might generally fall under lighter transparency obligations, the use of political bots in democratic processes, the focus of this research, is specifically addressed in Annex III of the AI Act as high-risk AI systems.⁴⁵¹ On the other hand, generative AI models are regulated as General Purpose AI (GPAI) models in the Act. Thus, generative AI-driven chatbots also need to be addressed alongside other risk categories related to political bots.⁴⁵²

Moreover, these transparency obligations are valid for chatbots and deep fakes.⁴⁵³ For instance, bots capable of correcting writing errors or predicting words during text input may also perform emotion recognition.⁴⁵⁴ Deep fakes are already being used for manipulative purposes during

⁴⁵¹ The list includes AI systems whose risks have already materialised or are likely to materialise in the near future. Moreover, the European Commission can expand this list by using various criteria and risk assessment methodology.

⁴⁵² A more detailed discussion of this issue can be found below under the section Generative AI-driven Political Bots and GPAI. See section 3.2.2.2. *Generative AI-Driven Political Bots and GPAI*.

⁴⁵³ Corrigendum to the position of the European Parliament Artificial Intelligence Act (n 444) Article 50.

⁴⁵⁴ 'Emotion Recognition Using Chatbot System', in Shraddha Pophale, Hetal Gandhi and Anil Kumar Gupta, *Advances in Intelligent Systems and Computing* (Springer Singapore 2021) <https://doi.org/10.1007/978-981-15-7234-0_54> accessed 26 July 2025.

election processes.⁴⁵⁵ They cause societal harms via manipulation of elections.⁴⁵⁶ In the AI Act, manipulative bots are prohibited, and bots engaging in emotion recognition are classified as high-risk.

However, AI-driven chatbots with emotion recognition capabilities can be used in democratic processes. As they will be used for political purposes, they will be defined as political bots. In that case, they would be considered high-risk AI systems as listed in Annex III. They should be classified under Annex III (8). Since they are used in the context of democratic processes. Therefore, a more detailed analysis of what it means for political bots to be classified as high-risk AI systems is provided below.

3.2.2.1. Political Bots as High-Risk AI Systems

The AI Act classifies political bots as high-risk AI systems when used in democratic processes, but several critical ambiguities limit the effectiveness of this categorisation. First, the Act does not provide a clear definition of “democratic processes,” which complicates understanding precisely the timing and parameters of democratic processes. Second, the exceptions outlined in Article 6(3) and Annex III create further confusion, raising doubts about the practical boundaries and applicability of high-risk classifications to political bots. Third, profiling is not only an integral part of political bots' core functionality but is also fundamental to nearly all AI systems deployed in political campaigns. Moreover, the exceptions defined by the AI Act for democratic processes explicitly do not apply in cases of profiling. Therefore, this raises a critical question: how can an AI system (for this research, political bots) designed for

⁴⁵⁵ ‘Artificial Intelligence, Democracy and Elections’ European Parliament (October 2023) <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI\(2023\)751478_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf)>.

⁴⁵⁶ Mariëtte van Huijstee and others, ‘Tackling Deepfakes in European Policy’ (European Parliamentary Research Service 2021) 33 <[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU\(2021\)690039_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf)>.

democratic processes realistically operate without engaging in profiling? Additionally, regulating AI systems in democratic processes implicitly treats these processes as commercial activities, potentially compromising fundamental rights and democratic values in favour of business interests.

The general framework for high-risk AI systems is set out in Article 6(1). However, Article 6(3) introduces an important qualification: AI systems listed in Annex III are not to be considered high-risk if they do not pose significant risks to health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making.⁴⁵⁷ For the categorisation of political bots as high-risk can be understood more directly through Article 6(2). According to Annex III, AI systems used in the context of democratic processes are explicitly listed as high-risk. Political bots, as digital tools used for political purposes during electoral processes, therefore fall within this category.

Article 6(3) provides a limited degree of flexibility in the classification of high-risk AI systems, but the number of restrictive criteria attached to it effectively limits the possibility of applying that flexibility in practice. For instance, as noted in Recital 53, some AI systems listed in Annex III might be used to improve the language of previously drafted documents for enhancing professional tone, academic style, or brand alignment. These systems are not designed to mimic human behaviour but rather to perform repetitive tasks more efficiently or with fewer errors. Their purpose is to support, not replace, human functions.

In contrast, the dynamics of political bots differ fundamentally from such productivity-oriented systems. Political bots are designed to mimic human users, convincingly so, often using large-

⁴⁵⁷ Corrigendum to the position of the European Parliament Artificial Intelligence Act (n 444) Article 6(3).

scale datasets to engage in seemingly authentic interactions. Political bots do not always operate visibly,⁴⁵⁸ nor do they always convey direct messages. If political bots were to engage in direct interaction while behaving like real humans, they would pose risks similar to those created when one human infringes upon the fundamental rights, safety, or health of another. However, in this case, the interaction does not occur between two natural persons or legal persons, but between an artificial conversational agent and a human user. Therefore, any potential rights violations or risks emerge between, at least, two fundamentally different types of actors. Additionally, the AI Act does not regulate human behaviour or AI itself, but rather the AI systems. This distinction is critical when assessing political bots under the Act.

On the other hand, Article 6(3) should also apply to political bots. Due to this provision, profiling renders the listed exceptions inapplicable and would likewise be relevant for political bots.⁴⁵⁹ In general, any AI system performing profiling will be classified as high-risk, regardless of other criteria or exemptions. This provision could potentially restrict the operational scope of political bots, as it questions whether they can function without engaging in profiling, a core aspect of their activities.

One of the key issues lies in the internal structure of Article 6(3), which refers ambiguously to “the first paragraph” and “derogation from paragraph 2.” These unclear references contribute to the overall complexity of the exception system introduced in Article 6(2). Also, these references make it difficult to interpret how exceptions to high-risk AI systems classification should be applied. This ambiguity undermines the legal clarity of the risk-based framework.

⁴⁵⁸ Doshi and others (n 32).

⁴⁵⁹ Corrigendum to the position of the European Parliament Artificial Intelligence Act (n 444) Article 6(3).

Also, it creates uncertainty around how political bots interact with other mechanisms in the Act, such as FRIA.

Furthermore, while Article 6(3) sets out conditions under which certain Annex III systems might be exempt from high-risk classification, Annex III itself contains further exceptions regarding AI systems used in democratic processes. Notably, for Article 6(3) exceptions to apply, only one of the listed conditions needs to be met, thus, a low threshold that further complicates legal certainty. This raises a fundamental question: when it comes to democratic processes, is the purpose of layering exception upon exception to create loopholes that stretch the boundaries of fundamental rights?

In Annex III, when political bots are 'intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda,' they are classified as high-risk AI systems.⁴⁶⁰ An exception to this includes AI systems to which natural persons are not directly exposed, such as tools used to organize, optimize, or structure political campaigns from an administrative or logistical point of view.⁴⁶¹

The purpose behind including optimization and logistics remains unclear and the Recitals provide no further explanation. As a result, AI systems employed in democratic processes can impact fundamental rights in ways that could pose significant risks of harm to fundamental rights such as Article 7 and Article 8 of the CFR. However, whether they will be classified as not posing a high risk remains unclear. The AI Act does not define 'significant risks of harm'.⁴⁶²

⁴⁶⁰ *ibid* Annex III (8).

⁴⁶¹ *ibid* Annex III (8).

⁴⁶² However, according to Article 7(2), the European Commission will consider criteria to decide whether the potential harm can be equivalent to or greater than the harm that can be caused by the AI systems in Annex III.

The most critical aspect of these exceptions is this: for an AI system to fall within the scope of the exception, natural persons must not be directly exposed to its outputs. However, there is no clear basis for assuming that indirect exposure poses a lesser threat to democracy, its principles, or the integrity of democratic processes. Even if the outputs of AI systems used in campaign logistics do not directly affect individuals, they can still shape the structure of political campaigns in ways that influence citizens indirectly.

For instance, optimising financial resources may involve deciding which regions to target. This could require profiling constituencies based on socioeconomic data. While this may offer strategic advantages to political parties, it simultaneously introduces targeted political engagement, raising fundamental rights concerns. Moreover, according to the guideline on AI systems definition, outputs are classified into four categories: predictions, content, recommendations, and decisions. Each of these involves a different level of human intervention. However, in practice, recommendations that are applied without further review may effectively become decisions. Given this, how can the indirect impact on individuals be dismissed when AI systems are used to optimise or organise the structure of political campaigns? These outputs, even if not directly targeting individuals, still shape how political messages are designed and delivered.

It is also worth noting that the exceptions are introduced with "such as," indicating that the list is non-exhaustive. Examples of indirect exposure could eventually resemble direct impacts, especially in sensitive contexts. For example, financial optimisation might guide resource allocation across electoral districts. In poorer districts, this may shape both political engagement and messaging, indirectly targeting specific populations. At that point, one must

ask: how does this relate to the Article 39 right to vote? Is the true aim of the provision really to protect individuals, or to safeguard the operational flexibility of political campaigns? Indeed, the AI Act attempts to clarify the purpose of Annex III (8) through Recital 62, which indicates that the aim is to protect the right to vote as articulated in Article 39 of the CFR. However, the regulation approaches democratic processes with a narrow perspective, reducing democracy exclusively to the right to vote.

The AI Act does not provide a definition of "democratic processes." Although democratic processes are inherently broad as a concept, the provision in Annex III (8) restricts itself to elections and referenda, themselves broad and complex terms. Yet, democratic processes differ significantly across member states. Local elections, general elections, presidential elections, and European Parliament elections each operate under different procedural, legal, and political conditions.

Therefore, the reference to "elections" could, as it stands, encompass every type of electoral process taking place within the EU. Such breadth endangers the provision's practical applicability. A concept so expansive cannot easily translate into effective and consistent regulation across diverse electoral systems. Furthermore, by limiting the scope to outcomes of elections and referenda, the AI Act fails to cover the full range of political activities and strategies. A core question remains unanswered: when do elections or referenda begin, and when do they end?

The text seems to acknowledge that democratic processes involve more than just election day outcomes. Indeed, while influencing electoral outcomes is explicitly covered in Annex III of the Act, political campaigns may cover different periods. It seems the AI Act recognises three

phases within democratic processes: (1) the campaign phase, (2) the exercise of the vote, and (3) the influence of outcomes. However, the Act only deems AI systems high-risk if they influence voting behaviour "in the exercise of the vote". This phrase lacks temporal clarity. Does it refer to election day itself, or does it include the broader campaign period? This research defines the democratic processes as the timeframe between the official announcement of the elections and referenda, and the moment the polls close on election day.

Still, it is important to remember that democratic processes cannot be reduced to voting behaviour alone. As discussed in Chapter 2, and drawing on Habermas, the formation of public political opinion depends on individuals being able to access and exchange accurate information freely. Political bots may contribute to information pollution and restrict public debate by silencing or overshadowing genuine voices.

The AI Act does not clarify when the period of democratic processes begins, ends, or how long it lasts. The lack of a definition of "democratic processes" may leave room for interpretation, however, political bots should not be excluded in this point. Historically, the AI Act's initial draft in 2021 offered words of "democratic processes," merely mentioning the term without elaboration. Given that democratic processes encompass far more than just elections or referenda, including broader participation rights and democratic representation, this ambiguity persisted through subsequent drafts, including the European Parliament's 2023 adopted version. Such lack of clarity exacerbated uncertainty around the regulation of political bots. Also, it implies that the regulation views democratic processes as part of a "business area."⁴⁶³ This conceptualization raises critical ethical and legal concerns, suggesting that fundamental rights

⁴⁶³ While the Act excludes high-risk classification for systems used before the official start of a campaign, this is when many strategic operations occur, including the setup and deployment of political bots. Thus, it shows that the AI Act is treating AI systems as part of a business ecosystem. Furthermore, its regulatory lens may prioritise market dynamics and operational efficiency over the protection of democratic values and individual rights.

and democratic values could become secondary to commercial interests, lobbying networks, profit-driven innovation, and continuity.

The sudden and impactful emergence of generative AI, particularly with OpenAI's ChatGPT in late 2023, represented a stress test for the AI Act, compelling it to revise its structural approach significantly. Consequently, new classifications such as General Purpose AI (GPAI) and systemic risks, as well as the FRIA, were introduced. These additions, intended as preventive mechanisms within AI-human interactions, ironically increased the Act's complexity. The growing number of mechanisms and compliance requirements has heightened concerns about the Act's practical implementation and overall efficacy.

In general, if it needs to focus on what a democratic process is, there is an action plan, “EU Action Plan on Human Rights and Democracy 2020-2024”, which promotes transparency of democratic processes⁴⁶⁴ and supports the policies that apply to offline election rules and democratic processes in the online context. It also promotes many action plans including plans against disinformation and European Democracy Action Plan and Digital Service Act (DSA) to build resilient, inclusive and democratic societies.⁴⁶⁵

Ultimately, the Act's original aspiration to foster innovation seems undermined by its complexity. Rather than providing clarity, the guidelines associated with AI definitions and regulatory mechanisms, as noted by critics like Kris Shrishak, have introduced further confusion.⁴⁶⁶ Thus, the AI Act, in its current form, appears insufficiently equipped to address

⁴⁶⁴ It highlights financing of political and issue-based campaigning by different actors. This issue is also highlighted by some participants in Chapter 4 section 4.6.3.1. *Democracy: An Overview*.

⁴⁶⁵ ‘EU Action Plan on Human Rights and Democracy 2020-2024’ 19 <<https://www.consilium.europa.eu/media/46838/st12848-en20.pdf>>.

⁴⁶⁶ Kris Shrishak, ‘EU’s AI Act: Tread the Guidelines Lightly’ Tech Policy Press (21 February 2025) <<https://www.techpolicy.press/eu-ai-act-tread-the-guidelines-lightly/>>.

future technological advancements and the nuanced realities of political bot usage within democratic processes.

In addition, Annex II of the Neighbourhood, Development and International Cooperation Instrument (NDICI)⁴⁶⁷ highlights strengthening and promoting democracy and inclusive democratic processes in cooperation areas for geographic programmes as well as transparent, inclusive and credible electoral processes and strengthening of a meaningful political participation and representation. The European Parliament officially adopted a committee⁴⁶⁸ report in March 2022 on “foreign interference in all democratic processes in the European Union”. The report concludes that misinformation and disinformation on social media is an increasing threat for electoral integrity. Moreover, the report calls attention to the lack of democratic oversight over the private sector.⁴⁶⁹

According to Recital 62 of the AI Act, unlike its draft versions, it is emphasized that provisions related to democratic processes must be implemented without prejudice to the rules provided for in TTPA and Article 39 of the CFR. The AI Act, applied with other relevant regulations, shows the significant effort to regulate digital devices and applications. This is due to the potential risk of foreign interference with democratic processes in the EU. Such interference reflects a broader threat to democracy across the Union.

⁴⁶⁷ Neighbourhood, Development and International Cooperation Instrument (NDICI) 2021 [2021/947].

⁴⁶⁸ This committee, as a special committee on foreign interference in all democratic processes in the EU, including disinformation, and defining its responsibilities, numerical strength and term of office, is decided to set up in June 2020. See Lukas Harth and Florian Kriener, ‘Responding to Foreign Interference in the EU: Beware of Unintended Consequences’ Carnegie Europe (10 December 2022) <<https://carnegieeurope.eu/2022/10/12/responding-to-foreign-interference-in-eu-beware-of-unintended-consequences-pub-88101>>.

⁴⁶⁹ ‘Foreign Interference in All Democratic Processes in the European Union. European Parliament Resolution of 9 March 2022 on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation.’ 30 <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.pdf>.

In conclusion, the AI Act introduces a multilayered regulatory framework characterised by numerous exceptions and further exceptions nested within these. While the Act explicitly classifies AI systems used in democratic processes, including political bots, as high-risk, the inherent complexity of its exception structure significantly contributes to uncertainty around their categorisation.

Political bots perform specific strategic functions in democratic processes, such as mimicking human behaviour, interacting with users and other bots, and disseminating political content to amplify narratives or spread disinformation. Although this analysis does not delve into the legal parallels of these functions found in other regulations, it highlights the importance of Recital 62. This recital clarifies how Annex III (8) should be interpreted in alignment with the TTPA, underscoring its significance in the legal framing of political bots.

3.2.2.2. Generative AI-Driven Political Bots and GPAI

In cases where political bots are driven by generative AI, the AI Act's provisions on GPAI also become relevant. Therefore, generative AI-driven political bots do not fit neatly into a single category within the legal framework drawn by the AI Act; instead, they intersect with multiple regulatory domains. The inclusion of GPAI provisions adds another layer of complexity to regulation.⁴⁷⁰ On the other hand, the rapidly evolving practices of political bot usage⁴⁷¹ further exacerbate doubts about the adequacy of the current framework.⁴⁷² Due to the complexity of

⁴⁷⁰ Hacker and others address this complexity as model-platform integration systemic risk which means AI systems embedded into large-scale platforms creating self-reinforcing feedback loops. See Philipp Hacker, Atoosa Kasirzadeh, and Lilian Edwards, 'AI, Digital Platforms, and the New Systemic Risk (Last Revised: 23 Sep 2025)' 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5475049>.

⁴⁷¹ This refers to the use of advanced technologies by political bots to avoid detection more effectively, as well as to the presence of other strategies serving similar aims. See more Doshi and others (n 32); Ferrara, 'Social Bot Detection in the Age of ChatGPT' (n 153).

⁴⁷² Leingang (n 248).

AI Act, and the potential for cumbersome bureaucracy when making amendments,⁴⁷³ concerns arise about the future effectiveness of this regulation.

Recital 99 explains that large generative AI models should be regarded as typical examples of General Purpose AI (GPAI). Recital 100 further clarifies that when a GPAI model is integrated into an AI system or its components, it is considered part of a GPAI system. Thus, political bots could also be classified as large generative AI models and, therefore, would be subject to the provisions regulating GPAI systems, as long as they are integrated into AI systems or their components.

However, GPAI models lead to systemic risks, which should also be examined in the context of political bots.⁴⁷⁴ The systemic risks of GPAI models embedded with political bots arise from issues such as misuse, reliability, fairness, and security. These risks also cover the facilitation of disinformation, threats to privacy, and harm to democratic values and human rights. Providers of GPAI models with systemic risk will continuously assess and mitigate systemic risks to take relevant and appropriate measures for the entire model lifecycle. Thus, a systemic risk management, which includes assessment, mitigation and update, ensure future proof lifecycle model.⁴⁷⁵

⁴⁷³ Mario Draghi, ‘The Future of European Competitiveness Part A | A Competitiveness Strategy for Europe’ (European Commission 2024) <https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en>.

⁴⁷⁴ Systemic risk, as a concept, is an outcome of the Great Depression and was later consolidated in financial literature. Hacker and others provide a table with a selected definitions of systemic risk (at 10). Considering AI systems deployed in democratic processes, the most reasonable definition might be Helbig’s: “Systemic risk is the risk of having not just statistically independent failures, but interdependent, so-called ‘cascading’ failures in a network of N interconnected system components.” This definition does not limit systemic risk to its financial dimension, and may therefore applicable to other potential risks as well. Philipp Hacker, Atoosa Kasirzadeh and Lilian Edwards (n 470) 6; Dirk Helbing, ‘Globally Networked Risks and How to Respond’ (2013) 497 *Nature* 51 <<https://doi.org/10.1038/nature12047>>.

⁴⁷⁵ Systemic risk management also requires establishing a risk culture. For this purpose, it requires a safety and security framework which requires risk identification, risk analysis, risk acceptance determination, safety and security mitigations and models, risk responsibility allocation and serious incident reporting. ‘Code of Practice for General-Purpose AI Models’ (European Commission 2025) <<https://ec.europa.eu/newsroom/dae/redirection/document/118119>>.

The state-of-the-art GPAI model, or another model with an equivalent level of influence, will pose systemic risks, but they can also include novel, previously unforeseen risks.⁴⁷⁶ Recital 110 explains that systemic risks include the dissemination of illegal, false, or discriminatory content as well as other risk factors. In the first General Purpose AI Code of Practice,⁴⁷⁷ the Code, mentions several types of risks,⁴⁷⁸ and one of them, clearly the most relevant to political bots, is the risk to fundamental rights.

Risks related to fundamental rights explicitly include risks to freedom of expression and information, and the democratic process, alongside other concerns. In addition, harmful manipulation, which is listed as a specified risk in the Code, can be directly associated with political bots.⁴⁷⁹ Harmful manipulation is the strategic distortion of human behaviour or beliefs. In this respect, political bots create such risks by targeting groups and populations or decision makers with persuasive, deceptive or personalised strategies.⁴⁸⁰ The Code itself highlights that such capabilities may erode democratic processes and fundamental rights, including by allowing the misuse of protected characteristics.⁴⁸¹ On the other hand, loss of control could be possible for political bots. For instance, there is the possibility of losing control over AI-driven

⁴⁷⁶ Artificial Intelligence Act (n 40) art 3 (65).

⁴⁷⁷ The document was released on 10 July 2025 since the AI Act rules applied from 2 August 2025. The code consists of three chapters: Transparency, Copyright, and Safety and Security. The last chapter, Safety and Security, provides an understanding of systemic risks for democratic processes by referring them in two places of the document. The document is presented as a voluntary tool, intended to support industry by assisting in design, reducing the regulatory burden on companies, and providing legal certainty. See ‘The General-Purpose AI Code of Practice’ EU Commission (9 September 2025) <<https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai#ecl-inpage-the-3-chapters-of-the-code>>.

⁴⁷⁸ These are risks to public health, risks to safety, risks to public security, risks to fundamental rights, risks to society as a whole. ‘Code of Practice for General-Purpose AI Models’ (n 475) 34.

⁴⁷⁹ *ibid* 37; Jelena Cupać and Mitja Sienknecht, ‘Regulate against the Machine: How the EU Mitigates AI Harm to Democracy’ (2024) 31 *Democratization* 1067, 1072 <<https://doi.org/10.1080/13510347.2024.2353706>>.

⁴⁸⁰ ‘Code of Practice for General-Purpose AI Models’ (n 475) 37.

⁴⁸¹ *ibid*.

political bots in unintended ways.⁴⁸² As a result, foreign interference in elections may not be limited to foreign actors. It is also possible that the autonomous behaviour of AI systems could unintentionally alter the direction or results of political campaigns beyond their original scope or intention.

The code listed specified risks based on the types of risks. Accordingly, the “high-impact capacities” listed in Appendix 1.2.1 of the Code as essential characteristics of risk are undoubtedly relevant to political bots. Almost all of the contributing characteristics listed in Appendix 1.2.2 of the Code can be applied to political bots. Namely, risks intensify as GPAI models gain reach (reach-dependent) and as their capabilities expand (capability-dependent). Moreover, considering the collective use of political bots as bot armies, high velocity becomes much possible. There is always a risk that GPAI models used as political bots may become irreversible or difficult to reverse during every election period, namely difficult or impossible to reverse risk.

Indeed, electoral processes are period-limited; once the ballot boxes are closed, electoral results are immediate and irreversible. Asymmetric impact is, moreover, inherent to political bots: the dissemination of information initiated by only a few bots, or the manipulative content shared with a limited set of users, already generates disproportionate effects. Together, these two features, which are irreversibility and asymmetry, make political bots require systemic risk assessment.

⁴⁸² Recital 110 provides this example. Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 152).

In addition, the Code identifies several sources of systemic risk, many of which are directly relevant to political bots. These include capabilities that may lead to persistent and serious infringements of fundamental rights, as well as the ability to manipulate, persuade, or deceive. Political bots also exhibit capacities closely tied to electoral strategies, such as long-horizon planning, forecasting, and strategizing. Finally, they may demonstrate self-replication, self-improvement, or modification of their environment, along with the capacity to process multiple modalities.

The Code also refers to model propensities in Appendix 1.3.2. For GPAI models operating as political bots, several are especially relevant: misalignment with human values (e.g. disregard for fundamental rights); a tendency to deploy capabilities in harmful ways (e.g. to manipulate or deceive); a tendency to hallucinate, produce misinformation, or obscure sources of information; and colluding with other AI models or systems.⁴⁸³

From the perspective of political bots, several points can be made:

1. Political bots themselves can cause large-scale societal harm.
2. Bots may be built upon today's most advanced LLMs.
3. Since 2016, while bot detection systems have become more sophisticated, political bots have also evolved in terms of strategy. This suggests that novel risks may emerge through political bots.

Moreover, even if a GPAI model is not technically classified as one of the “most advanced models,” it may still pose systemic risks due to its scale, reach, or the way it is embedded into broader infrastructures (e.g., scaffolding mechanisms). This exceptional framework should be

⁴⁸³ ‘Code of Practice for General-Purpose AI Models’ (n 475) 36.

taken into account in the systemic risk assessment of political bots, even if they do not pose risks at the state-of-the-art level.

Also, Recital 110 highlights that international approaches need to pay attention to systemic risks, in particular the potential for democratic values and human rights. The AI Act does not include references to any related regulations regarding democratic values, nor does it explicitly define democratic processes. Still, political bots have the potential to pose systemic risks in relation to democratic values and fundamental rights. However, a definition of what is meant by democratic processes is still missing from these documents.

As the AI Office decides which models can be assessed as GPAI models. For this purpose, the Code of Conduct, composed of three separately authored chapters. These documents adopt international approaches as mentioned in Article 56(1), which will be valid for political bots. This risk framework for political bots raises awareness and builds a safety culture. However, the two additional layers described below could create excessive paperwork, reducing the process to a box-ticking exercise. In conclusion, the Code of Practice provisions related to GPAI may have reduced some uncertainties, but they still do not provide a clear framework in the AI Act regarding political bots.

3.2.2.3. FRIA for Political Bots

For political bots, the AI Act introduces three layers of assessment: conformity assessment, FRIA, and systemic risk assessment. Yet, the assessments primarily focus on the AI product⁴⁸⁴ because the risk assessments tend to concentrate on system design, often even the system

⁴⁸⁴ Alessandro Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 Computer Law & Security Review 106020, 7 <<https://doi.org/10.1016/j.clsr.2024.106020>>.

architecture or model's architecture.⁴⁸⁵ However, AI systems are better understood as socio-technical systems, where design emerges through continuous interaction and reciprocal modification in society.⁴⁸⁶ Political bots have already been used to manipulate individuals to influence political opinions, as is well-known due to the Cambridge Analytica scandal. They cause many risks, including harming the democratic process⁴⁸⁷ as AI systems, political bots shape democratic preferences and processes.⁴⁸⁸ On the other hand, the multi-layered risk assessments and conformity assessment structure risks complicating and delaying effective risk management. As a result, assessing the impact of AI on fundamental rights will require a stronger methodological approach.⁴⁸⁹

Accordingly, political bots placed in the high-risk category complete two main obligations: a conformity assessment and a FRIA.⁴⁹⁰ Where a GPAI model is embedded, they are also subject to an additional systemic risk assessment.⁴⁹¹ The key distinction here is that FRIA is to be completed by deployers, whereas systemic risk assessment and the conformity assessment fall to providers.

The conformity assessment consists of determining whether the AI system qualifies as high-risk, which -in this case for political bots- it does, and of evaluating the risks that form part of the risk management system.⁴⁹² The purpose of the conformity assessment is to ensure a high-

⁴⁸⁵ 'Code of Practice for General-Purpose AI Models' (n 475) 3 and 19.

⁴⁸⁶ Mantelero (n 484) 7.

⁴⁸⁷ Risto Uuk, 'Manipulation and the AI Act' (The Future of Life Institute 2022) 5.

⁴⁸⁸ Mariano-Florentino Cuéllar and Aziz Z. Huq, 'The Democratic Regulation of Artificial Intelligence' (*Knight First Amendment Institute at Columbia University*, 31 January 2022) 24 and 25 <<https://knightcolumbia.org/content/the-democratic-regulation-of-artificial-intelligence>>.

⁴⁸⁹ Mantelero (n 484) 7.

⁴⁹⁰ Artificial Intelligence Act (n 40) art 27.

⁴⁹¹ *ibid* 55.

⁴⁹² Andreea Serban, Vasileios Rovilos and Katerina Demetzou, 'Conformity Assessments under the EU AI Act: A Step-by Step Guide Updated with the Final Text of the AI Act' (Future of Privacy Forum and OneTrust LLC 2025) White Paper 8 <<https://fpf.org/wp-content/uploads/2025/04/OT-comformity-assessment-under-the-eu-ai-act-WP-1.pdf>>.

level trustworthiness of high-risk AI systems,⁴⁹³ and to prevent or at least mitigate relevant risks. However, FRIA, by contrast, considers mitigation only when prevention is not feasible.⁴⁹⁴

Therefore, the starting point is to identify the risks that stem from the political bots and their operations. Even when political bots are not part of an electoral strategy, they still create data privacy risks through their data gathering capabilities on platforms and large-scale training. However, when political bots are specifically deployed as part of an electoral strategy, risk identification becomes more diverse. For instance, risks of disinformation, lack of transparency, discriminatory bias, a tendency to produce misinformation, and disregard for fundamental rights will be required to identify.

Both conformity assessment and FRIA follow similar steps such as risk identification, analysis, and prevention or mitigation. As Mantelero highlights, both procedures rest on a general risk management methodology.⁴⁹⁵ However, conformity assessments are standard based approach, and FRIA is characterised as right-based approach.⁴⁹⁶ Thus, conformity assessment is a tool for enhancing consistency within the EU Market under the New Legislative Framework. However, conformity assessment does not directly address fundamental rights, it will not be considered in this research.⁴⁹⁷

⁴⁹³ Artificial Intelligence Act (n 40) Recital 123.

⁴⁹⁴ Mantelero (n 484) 6.

⁴⁹⁵ *ibid.*

⁴⁹⁶ *ibid* 5.

⁴⁹⁷ It requires product compliance and the provider to establish a quality management system, rely on the technical documentation to assess compliance, and ensure consistency in the system's design and development process.

The AI Act does not provide specified structure and implementation methodologies for FRIA.⁴⁹⁸ This is because the FRIA approach generates conceptual and normative issues that affect the current system of the protection of human rights by autonomous agents.⁴⁹⁹ Thus, while a FRIA tailored to democratic processes remains far from clear, what can be understood at its core is the need for risk management and risk culture awareness. For FRIA, in the case of AI systems used in democratic processes, namely political bots, three elements are crucial: identifying the fundamental rights most affected by their use in democratic processes (Article 7, Article 8, Article 11 and Article 39 of the CFR); defining the components of political bots (such as training data, algorithm, and interface); and outlining the parameters and features that determine its impact on fundamental rights.⁵⁰⁰

3.2.3. Specific Regulatory Dimensions Applicable to Political Bots

3.2.3.1. Mimicking Human Users

Political bots are, first and foremost, bots. They must fully comply with transparency obligations under the AI Act.⁵⁰¹ Since the very beginning of the AI Act's regulatory process, they have been required to comply with transparency obligations, regardless of whether they mimic human behaviour or not.⁵⁰² These transparency requirements remain under the final version of the Act.⁵⁰³

⁴⁹⁸ Lucilla Gatt and others, 'FRIA Implementation Model According to the AI Act' *2024 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRINE)* (IEEE 2024) 1228 <<https://doi.org/10.1109/MetroXRINE62247.2024.10796624>> accessed 24 September 2025.

⁴⁹⁹ *ibid.*

⁵⁰⁰ Gatt and others refer to the "judicial sector" in their work, but this research deliberately avoids describing democratic processes as sectors. This is because framing democracy as a sector would detach it from its normative and conceptual ideal. *ibid* 1225.

⁵⁰¹ Cupać and Sienknecht (n 479).

⁵⁰² Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts 2023.

⁵⁰³ Article 50 Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (n 152).

Political bots that mimic human users typically begin by presenting themselves as egg accounts. Namely, they have profiles without photos, often display the default profile picture on the social media site of an egg.⁵⁰⁴ Also, political bots may purchase followers to enhance credibility, a widespread strategy. They then proceed to post using targeted hashtags, phrases, or keywords.⁵⁰⁵ These behavioural patterns, as noted above, are among the key indicators used to detect bot activity. Political bots proceed to post using targeted hashtags, phrases, or keywords.⁵⁰⁶ Their common behavioural patterns, as noted above in Chapter 1, are among the key indicators used to detect bot activity.

As detection systems have improved, political bots have adapted their strategies to avoid being identified with the help of advancing technologies.⁵⁰⁷ The behavioural patterns of newer generations of political bots have become more sophisticated.⁵⁰⁸ One particularly striking example is the use of real human photos and personal data to create bot accounts and disseminate content. However, such activity does not fall under the definition of deepfakes.

Deepfakes refer to AI-generated or AI-modified media content, including images, videos, and audio recordings.⁵⁰⁹ They often appear indistinguishably real. This hyper-realistic synthetic content is typically powered by advanced generative AI, particularly through the use of Generative Adversarial Networks (GANs). Generally, deepfake production follows two main

⁵⁰⁴ Howard, Woolley and Calo, 'Algorithms, Bots, and Political Communication in the US 2016 Election' (n 427) 83.

⁵⁰⁵ Papakyriakopoulos (n 222); Daniel Kreiss, 'Micro-Targeting, the Quantified Persuasion' (2017) 6 Internet Policy Review <<https://doi.org/10.14763/2017.4.774>> accessed 13 February 2024.

⁵⁰⁶ Chu and others (n 370).

⁵⁰⁷ Schellekens (n 399).

⁵⁰⁸ Ferrara, 'Social Bot Detection in the Age of ChatGPT' (n 153).

⁵⁰⁹ In this definition, "media" appears an important distinction. According to the definition, AI-generated text outputs do not fall within the scope of this provision. European Parliamentary Research Service, 'Children and Deepfakes' *European Parliament* (July 2025) 2 <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf)>.

approaches: the first involves transforming existing media and generate entirely new content from scratch using AI models, such as image-generation systems. The second common method, frequently used in tasks like face-swapping, relies on autoencoders.

In 2023, approximately 500,000 deepfakes were circulating online. This number is projected to rise dramatically, with estimates pointing to 5 million by 2025.⁵¹⁰ Thus, deepfakes introduce significant risks and disruptions across a range of domains, from politics to journalism by mimicking authenticity and distorting perception. However, political bots use or disseminate natural persons photos as profile pictures. This activity is not described as a deepfake characteristic because there is no manipulation or modification on authentic content.

According to Article 3(60) of the AI Act, three criteria must be met for content to be classified as a deepfake: (1) the content must be AI-generated or manipulated by an AI system; (2) the generated or manipulated content must resemble an existing person,⁵¹¹ object, entity, place or event; and (3) it causes a false sense of authenticity to the viewer.⁵¹² As highlighted in the definition in Article 3(60) of the Act, a key characteristic for detecting this kind of content is that it falsely appears to a person to be authentic or truthful. However, the political bots' practice of scraping real images and using them without modification, under false names or identities to mimic human users, does not satisfy all three conditions. Since the content is not altered or generated, but merely repurposed, this activity is better understood as account impersonation or identity deception, not as a deepfake creation.

⁵¹⁰ *ibid* 1.

⁵¹¹ The reference to an "existing person" in the definition of a deepfake is particularly significant, because political bots may use generated profile images which belongs non-existent personas. This distinction is assessed below. See next paragraphs.

⁵¹² Artificial Intelligence Act (n 40) art 3(60).

These earlier strategies, which were adopted by political bots appear obsolete. As generative AI becomes widely available, it has become increasingly common for political bots to use profile images which belongs non-existent personas. The datasets used to train these models, political bots, enable them to generate images of individuals who do not exist. In addition, other profile details, such as usernames, personal names, geographical locations,⁵¹³ and biography texts, are also frequently generated using LLMs. These activities of political bots serve a clear purpose which is to enhance credibility and to convincingly mimic human users. Moreover, they can appear more realistic and align with terms of conditions of the platforms. Thus, they increase the likelihood of engaging with real users and make detection significantly more difficult. In this case, it is quite clear that generated and used content by political bots does not belong existing persons, thus this activity is not related to deep fakes.⁵¹⁴

3.2.3.2. Interaction with Natural Persons

A fundamental characteristic of political bots is their interaction with humans. Initially, political bots were specifically created as controlled and managed tools designed primarily to manipulate public opinion. The interactions they perform can occur in two main forms: interaction with natural persons (humans) and interactions among bots themselves. While bot-to-bot interactions will be examined separately within the AI Act's framework, this section specifically addresses interactions between political bots and natural persons.

⁵¹³ User locations can be inferred from tweet metadata. Even in the absence of a dedicated system, it is still possible to automatically infer user locations from analysing metadata of the tweets. Alp Önder Yener, Ali Najafi and Onur Varol, 'City-Level User Location Detection from Social Media and Analysis of Political Participation' *2024 32nd Signal Processing and Communications Applications Conference (SIU)* (IEEE 2024) <<https://doi.org/10.1109/SIU61531.2024.10600825>> accessed 8 September 2025.

⁵¹⁴ However, one of the ongoing debate about the use of generative AI-driven political bots is their training with a huge amount of datasets. Since these datasets include personal data of natural persons, generated or manipulated profile pictures, user accounts and content is quite easy for political bots. However, this concern is closely linked to deepfake concept and copyrights, as generated content is based on natural persons' data, while it remains nearly impossible to detect the specific person it was derived from. Due to this link, this matter falls out the scope of this research project, additionally, the AI Act.

Interactions with natural persons are considered high-risk. This interaction may take many forms, but the first and most essential point is that, according to the transparency obligation under Article 50, natural persons must be clearly informed that they are engaging with a bot. In addition, if the system performs profiling, this triggers the full set of obligations applicable to high-risk AI systems, including documentation requirements, systemic risk assessments, and, crucially, the obligation to conduct a FRIA under Article 27.

Specifically, Article 27(1)(b) requires deployers to indicate the frequency with which each high-risk AI system is intended to be used. In the case of political bots, this is particularly difficult to establish, as their activities are often rapid, unpredictable, and large in volume. Similarly, under Article 27(1)(c), deployers must define the categories of natural persons and groups likely to be affected by the system in its specific context. This is also highly challenging for political bots, as it is difficult to determine who exactly will be targeted, at what scale, and whether those individuals are considered vulnerable.

Furthermore, according to Article 27(1)(e), the measures to be taken in case the risks materialise must be clearly outlined. From the perspective of democratic principles, this should require deployers to transparently disclose their risk mitigation strategies and provide clear criteria for assessing those risks. They must release these strategies during democratic processes to ensure timely precautions.

Additionally, a further clarification related to deepfakes is necessary. As previously mentioned, the definition of deepfake content is explicitly limited to media content, as outlined in Article 3(60) of the AI Act and other related EU documentation. This distinction regarding media content is crucial. Similar to media content, textual outputs produced by AI systems fed with large datasets result in language use patterns. Such outputs might not always be accurate or unbiased, and the impartiality of the information provided can be compromised. Indeed, it is

well documented that consecutive interactions can lead models to respond with decreasing confidence.

Political bots generate synthetic conversations that do not fit within the definition of deepfakes because deepfakes specifically apply to media-based content. However, conversations inherently occur between humans, whereas content generated by political bots remains synthetic and inherently one-sided. Therefore, these interactions cannot be genuinely considered conversations under this strict definition. Although not categorised as deepfakes, bot-generated interactions cannot accurately be classified as conversations, as conversations by definition imply authentic human-to-human communication.

As a result, interactions involving political bots may, in some cases, contribute to the dissemination of accurate political information. This would, in fact, indicate that such bots are being used for constructive purposes. In some other cases, the only requirement under the AI Act becomes important. Users must be clearly informed that they are interacting with a bot. This requirement, however, fundamentally alters the nature of political bots. These bots are specifically designed to mimic human users, which is their core strategy. While transparency obligations are necessary from a legal and ethical standpoint, they also undermine the very function political bots are meant to serve.

3.2.3.3. Spreading AI-Generated Content

Providers of political bots will be responsible for spreading AI-generated content. This responsibility relies on Article 50 of the AI Act. In line with Recital 134 in the Act, providers are required to ensure that content generated or manipulated by AI is clearly and intelligibly labelled as artificially generated or modified. In Article 3 (3), provider develops AI system or a GPAI model. Namely, provider refers to the developer of the political bot. However, the scenarios may vary according to bots' functions.

In the case of political bots, the question of who describes as the provider⁵¹⁵ can be reassessed across different scenarios. The first scenario would be an individual user develops a political bot using Python, the LLaMA API,⁵¹⁶ or another model and deploys it on a platform. In this case, the provider would be the person who both develops and uses the bot for his own account or accounts. Thus, this person will be developer, and deployer. In this scenario, political bots may present as open to public interaction, thus, the provider will also be distributor. Besides the transparency obligations for each bot, including political bots, this time the requirements for high-risk AI systems will be filled by distributor. According to Article 24(3) of the AI Act, distributor will ensure that follow Section II of the AI Act.

Second scenario would be to build bot on top of a foundation model. For example, Meta's LLaMA, OpenAI's GPT, or Claude. For this case, provider of this model will be a GPAI provider. However, when the model is taken and used for political purposes such as political bots, the person or entity operating the bot becomes the AI system provider. Another example would be the integration of an OpenAI GPT-4-based chatbot into a platform such as X. GPT-4 is a general-purpose LLM developed by OpenAI. If this model is used to set up a bot on X for influencing political public opinion in favour of a political party or political campaigns, several roles emerge. First, OpenAI remains the GPAI model provider and, by making the

⁵¹⁵ According to the AI Act, the definition of "provider" in Article 3(3) is quite broad. First, A provider can be a natural or legal person, a public authority, an agency, or another type of body. Then, these actors may actors may qualify as providers if they develop an AI system or a general-purpose AI model, if they have such a system or model developed and place it on the market, or if they put the AI system into service under their own name or trademark, whether for payment or free of charge. See Article 3(3) in Artificial Intelligence Act (n 40).

⁵¹⁶ This service is provided by Meta for now and allows developers to integrate powerful Llama models into their own applications, tools, and services. APIs allow software developers to customise and quickly integrate a piece of technology into their own products. Kenrick Cai, 'Meta Introduces Llama Application Programming Interface to Attract AI Developers' *Reuters* (29 April 2025) <<https://www.reuters.com/business/meta-introduces-llama-application-programming-interface-attract-ai-developers-2025-04-29/>>.

model publicly available, is responsible for any kind of outputs including errors, threats, or disturbing responses.

However, when a general-purpose model such as GPT-4 is integrated into an AI system for a specific purpose, such as generating political content or enabling political interactions on a particular platform, the person who deploys the system on that platform also qualifies as a provider. Furthermore, if the bot is developed for a third party, such as for use in a political campaign or by a political party, then those parties or campaigners would be considered deployers under the AI Act.

In these scenarios, the responsibility of the provider is outlined in Article 50(1) of the AI Act. From the outset, the AI Act's proposed solution to behaviours that mimic human intention, such as those performed by political bots, has been the imposition of transparency obligations. Where AI systems are intended to interact directly with natural persons, they must be designed in a way that allows individuals to understand that they are interacting with an AI system. This responsibility is explicitly assigned to the provider.

Accordingly, when providers make political bots available, they are required to inform users that they are engaging with a bot.⁵¹⁷ However, since political bots are designed to mimic human behaviour, the application of the transparency obligations under Article 50 would, in effect, require altering the very nature of them, as concluded above as well.

⁵¹⁷ This point has also been addressed in Section 2.3.2, Interaction with Natural Persons.

3.2. The reflection of the DSA on political bots

This section focuses on the extent to which the Digital Service Act (DSA)⁵¹⁸ contributes to contrasting the phenomenon of manipulative bots from the perspective of political bots. It also explores whether the transparency requirements of the DSA are adequate to protect democratic processes from the spread of disinformation. As Farrand explains, the DSA does not mention political advertising specifically, instead the Act sets out procedures about “illegal/risky” content.⁵¹⁹ However, the Act provides a regulatory framework for online platforms and it is complemented by the TTPA and Strengthened Code.⁵²⁰

The implementation of the DSA could raise several challenges regarding bots, particularly political bots. This is because bots can function as content creators. They may also be used in the provision of intermediary services. Thus, bots can direct user interaction, distribute content, or influence user behaviour. In doing so, they could fall within the scope of the DSA.

After the ChatGPT revolution,⁵²¹ the legal framework still navigates around legal gaps, despite the AI Act, the DSA,⁵²² and even the TTPA.⁵²³ This is because, DSA is not designed to address content created by generative AI, as such systems fall outside its scope of application.⁵²⁴ In

⁵¹⁸ The DSA, enforced across the European Union from February 17, 2024, provides digital services to adhere to specific rules for creating a safer digital space and securing a predictable, trusted online environment at the same time. briefly, online content moderation is governed by the Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (n 167).

⁵¹⁹ Benjamin Farrand, ‘Regulating Misleading Political Advertising on Online Platforms: An Example of Regulatory Mercantilism in Digital Policy’ (2024) 45 Policy Studies 730, 740 <<https://doi.org/10.1080/01442872.2023.2258810>>.

⁵²⁰ ‘The Strengthened Code of Practice on Disinformation 2022’ (n 193) 202.

⁵²¹ Bassini (n 161) 2.

⁵²² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (n 167).

⁵²³ Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (n 41).

⁵²⁴ European Commission, ‘Commission Recommendation (EU) 2023/2829 of 12 December 2023 on Inclusive and Resilient Electoral Processes in the Union and Enhancing the European Nature and Efficient Conduct of the Elections to the European Parliament’.

other words, the DSA does not cover either AI systems or AI-generated outputs. As for TTPA, this regulation only focuses on identifying who is behind the paid advertising rather than the specific activities of political bots. Moreover, Meta and Google have announced that they will not provide paid political advertising services in the EU in order to avoid complying with the requirements of the TTPA.⁵²⁵ As a result, this may possibly lead to an increase in the activities of political bots. Additionally, this point can be summarised as follows: the EU's legal framework for AI-driven models and systems will lead to the further uncontrolled proliferation of political bots.

Accordingly, if AI-generated speech were meant to be regulated under the DSA,⁵²⁶ it would already have been done, but it has not. This creates a legal gap that cannot be resolved simply by extending existing rules or legal frameworks. This is because if the rule makers had intended to extend the regulation into not regulated circumstances, this would have been done through legislation.⁵²⁷ Moreover, the recent adoption of both instruments, DSA and AI Act, indicates that any flexible approach would fall outside the purpose of the regulation. From this point on, the only reasonable solution, short of legislative amendment, lies in the potential breadth of the ECtHR's interpretation of freedom of expression, and the extent to which this interpretation can be applied through the CFR.

The DSA provides tiered structure in four classes which are providers of online intermediary services, providers of hosting services, online platforms and very large online platforms

⁵²⁵ Annette Kroeber-Riel (n 390); META, Newsroom for Europe, Middle East and Africa (n 359).

⁵²⁶ The Digital Service Act, which as of 17 February 2024 applies to all platforms, regulates harmful disinformation or undesirable machine-generated speech that can be blocked by using automated filters or relevant tools. Nevertheless, the DSA can lead to censorship or over-blocking.

⁵²⁷ As Bassini also notes, US scholars have engaged more extensively with the questions of whether machine speech can or should be regulated or protected. However, EU regulations ultimately emerge in response to the needs voiced by academic and legal circles. Bassini (n 161) 11.

(VLOPs) with very large search engines (VLSEs).⁵²⁸ There would be primary importance of the DSA for democratic processes in three dimensions. First, providers of digital services are obligated to hire content moderators to check content and detect illegal content.⁵²⁹ Namely, bot-created content will be moderated. Second, the providers of digital services must ensure transparency for any advertisement. Thus, providers should provide transparency for targeted political advertisements as well. Indeed, such transparency requirements have already been regulated under the TTPA. However, the main contribution of the TTPA is to inform users about who financed a paid political advertisement. For DSA, transparency constitutes a central principle.⁵³⁰ From the digital public sphere perspective, DSA regulates that terms and conditions of VLOPs and VLOSEs must be articulated in plain and intelligible language. So, VLOPs and VLOSEs providers are required to disclose advertising details transparently to the users of their digital services. The providers of VLOPs and VLOSEs are prohibited from presenting advertisements that rely on profiling. Nevertheless, bots can still be programmed to employ diverse algorithms that process information provided by digital services such as X (previously known as Twitter), including gender, location, and political preferences.

⁵²⁸ As of 2023, the European Commission released the list of the VLOPs and VLSEs, accordingly, 17 VLOPs such as TikTok, YouTube, Snapchat and 2 VLSEs which are Bing and Google Search have been listed as meeting the criteria and operating in the EU. These platforms have been used by at least 45 million active users every month based on their user data. This is why they have to comply with the requirements of DSA. 'Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines' [2023] *European Commission-Press release* <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413>.

⁵²⁹ It seems content moderation can be an automated activity, or not, to detect, identify and address the illegal content. Illegal content is defined in the DSA but this definition does not cover any activity regarding disinformation. In DSA, Recital 3 addresses the rise of online disinformation. Instead of the regulation, DSA, the guidelines for the providers of VLOPs and VLSEs on the mitigations of systemic risks for electoral processes pursuant to the DSA highlights disinformation as well as measures, red-teaming and deepfakes. European Commission, Annex to the Communication to the Commission Approval of the content of a draft Communication from the Commission on Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to the Digital Services Act (Regulation (EU) 2022/2065) 2024.

⁵³⁰ The DSA defines advertising as promoting the message of either a natural or legal person. Also, whether for commercial or non-commercial objectives, this distinction is not considered significant for the advertising definition. See Recital 45, Recital 48, Recital 49 in DSA. Also see Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (n 167) ch 3.

This also raises an important question: should providers be expected to ensure the same transparency level for political advertisements generated or disseminated by political bots? If so, important ambiguities arise regarding political bots. It remains uncertain whether political bots operate in exchange for remuneration, whether their ordinary communicative activities can qualify as advertisements, and how this distinction can be determined in practice. The DSA defines an “advertisement” as information presented on an online platform against remuneration for the purpose of promoting a message, irrespective of whether the purpose is commercial or non-commercial.⁵³¹

As a result, providers are expected to ensure the same transparency for political advertisements, even those generated by political bots. This requirement stems from DSA's definition of 'dissemination to the public' as the act of making information available to a potentially unlimited number of third parties. Consequently, providers of VLOPs and VLSEs are obliged to implement new systems for the detection of illegal content and take appropriate action, in addition to increasing the transparency and accountability of content moderation.

For the third category of systemic risks concerns the actual or foreseeable negative effects on democratic processes, civic discourse, electoral processes, and public security. Thus, the DSA regulates recommender systems, including profiling activities which means protecting the users that bots or political parties target during electoral process. The DSA highlights electoral processes in Article 34 on risk assessment. It requires providers of VLOPs and VLSEs to identify and assess systemic risks arising from their services, including algorithmic systems. In particular, Article 34(1)(c) addresses actual or foreseeable negative effects on civic

⁵³¹ *ibid* 3(1)(r).

discourse, electoral processes, and public security. This provision is especially significant for political bots and manipulative digital communication.

From the perspective of political bots, one positive aspect of the DSA is the obligation for providers to disclose how recommender systems operate and which main criteria they use. But, it does not mandate the disclosure of the identity of trader or additional details of promoted political advertisements. The identity of the trader is required to be revealed only if the content is considered illegal. Therefore, any illegal content⁵³² disseminated⁵³³ during a democratic process can be identified, blocked, and moderated according to DSA. However, the issue of disinformation remains a concern, as it may not always fall under the category of illegal content.

According to the European Democracy Action Plan, three criteria are provided to define disinformation which are creating inaccurate information, intention to spread the content, potential to cause public harm. False or misleading content spread with an intention to provide economic or political gain and may result in public harm. The content may be defined as illegal in a member state of the EU but the immersive and sudden influence on voters can result in inalterable outcomes. Thus, disinformation, as harmful content, may fall into the systemic risk category of the DSA, due to potential systemic effects, such as the erosion of trust in democracy and institutions. For this reason, a mitigated risk approach of VLOPs may be required.⁵³⁴

⁵³² Under the DSA, “illegal content” refers to any information that, in itself or in relation to an activity, is not in compliance with Union law or the law of a Member State that complies with Union law. See details *ibid* 3(1)(h).

⁵³³ As mentioned above, the DSA defines “dissemination to the public” as making information available to a potentially unlimited number of third parties at the request of the recipient of the service who provided the information. *ibid* 3(1)(k).

⁵³⁴ Miriam Buiten, ‘Combating Disinformation and Ensuring Diversity on Online Platforms: Goals and Limits of EU Platform’ [2022] SSRN Electronic Journal <<https://doi.org/10.2139/ssrn.4009079>> accessed 1 March 2024.

On the other hand, the EU needs to ensure balance between what exactly the online safety by moderating content that is produced by bot accounts, and freedom of expression.⁵³⁵ Content moderators moderating or deleting statements made by political bots could potentially conflict with the principles of free speech and information. This is challenging because imposing restrictions on freedom of speech and information via content moderators, particularly during elections, can hinder the development of a democratic culture of debate, making it hard to justify such measures as proportionate.

Furthermore, the content may be defined as illegal in a member state of the EU but the immersive and sudden influence on voters may not be reversible. On the other hand, shared content in the EU can be defined as illegal in non-EU country and still cause influence on the voters during the democratic process. This is why the DSA may not provide real protection to individuals during democratic processes because of content that is created or promoted via political bots.

Bots possess the ability to create and distribute content, which will be subject to the content moderation policies of VLOPs and VLOSEs. However, bots can promote political discourse, opinion, comment or any political content. According to DSA, consumers⁵³⁶ can be any natural person, and traders⁵³⁷ are both, natural person and legal person. However, bots are robots without any persona that has been approved by legal systems, nevertheless, bots still can produce and share content. This is why DSA does not cover bots as traders or consumers. However, the DSA defines online platforms⁵³⁸ as hosting services which store and disseminate

⁵³⁵ *ibid* 18.

⁵³⁶ Article 3 (c) ‘Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines’ (n 528).

⁵³⁷ Article 3 (f) *ibid*.

⁵³⁸ Article 3(i) *ibid*.

information to the public. Bots are automated robots which are designed to complete various tasks. Therefore, bots can function as online platforms or perhaps part of an online platform if they are designed to store information, which is one of its tasks and an integral part of bots' core task.⁵³⁹

In terms of the definition of 'online interface' in the DSA, which means any software, various platforms such as websites, individual web pages, applications, and mobile applications are covered by this definition. For instance, an AI chatbot embedded within an online retail store's webpage serves as an online interface. Customers can interact with this bot to inquire about product details, check the status of their orders, or receive recommendations based on their shopping history. These bots are designed as software that users can interact with directly on a website or via applications on different devices. In this scenario, bots should be conceptualised as software, otherwise an automated robot with script-completed tasks may be out of this scope. Therefore, the classification of a bot as an online interface relies on its ability to function as software that facilitates interaction with users. Upon exploring the categorization of bots under the DSA, it is evident that the most fitting classifications based on their functions are "online interfaces" or "online platforms". Nonetheless, categorising bots as traders or consumers is not applicable.

3.3. Could the CFR Provide Further Protection Against Political Bots?

Bots are robots without any legally recognized persona. However, bots are still capable of acting as real person accounts on digital platforms such as X, Telegram, Facebook, Instagram, etc. Bots generate and disseminate multiple forms of content, even if this content is not entirely

⁵³⁹ For a discussion on micro-platforms, see Section 2.2.3, "As Digitalization Transforms Media, What Is the Role of Political Bots in New Media?".

accurate, individuals can access this content. For this very reason, Chapter 2 engages with Habermas's public sphere theory from the perspective of political bots. As Habermas also emphasises, digital social networks have been freedom-promoting.⁵⁴⁰ However, the right to freedom of expression was primarily intended to protect citizens from state prohibitions,⁵⁴¹ not to extend this protection into the private sphere.⁵⁴²

This raises questions about whether people should have the right to access false information, and if so, whether this right should be limited or if false information should be outright banned. On the other hand, there would be a consideration as to who decides what constitutes false information and what criteria define accuracy. As discussed in Chapter 2, the press has a well-established role as a public watchdog. However, since new media has developed a business model that competes with traditional media, the quality of professional information has become a serious concern.⁵⁴³ This is precisely where the question of accuracy arises. As debates on free speech highlight, it is contested who gets to determine what speech is acceptable or unacceptable, namely, good or bad. Thus, this raises further question of information could also be approached in a similar way. Ultimately, can it be argued that people have the right to decide for themselves what information they decide to believe?

⁵⁴⁰ Frank Dietrich, 'AI-Based Removal of Hate Speech from Digital Social Networks: Chances and Risks for Freedom of Expression' (2025) 5 *AI and Ethics* 2943, 3 <<https://doi.org/10.1007/s43681-024-00610-7>>.

⁵⁴¹ Articles 11 and Article 53 of the CFR mandate EU Member States to fulfil both negative and positive obligations. To meet the negative obligations, States are required to refrain from interfering with the scope and use of these rights, with permissible exceptions for interference outlined only in Article 10 of the ECHR. Positive obligations necessitate protecting individuals' freedom of speech, with a particular focus on upholding media pluralism as a significant responsibility of the State. Charter of Fundamental Rights of the European Union (n 39) arts 11 and 53.

⁵⁴² As Rowbottom discusses, the "more speech the better" view contributes to the formation of public opinion in the public sphere. However, regarded as a democratic ideal by Rowbottom, the independence of public opinion could only be realised as a matter of degree. Jacob Rowbottom, 'Government Speech and Public Opinion: Democracy by the Bootstraps' (2017) 25 *Journal of Political Philosophy* 22, 22, 31 and 47. <<https://doi.org/10.1111/jopp.12101>>; Dietrich (n 540) 3.

⁵⁴³ Bassini (n 161) 6.

Even when content generated or disseminated by bots does not align with reality or contains inaccuracies, it still warrants protection under the scope of freedom of expression and information.⁵⁴⁴ The next section will explore how these issues are balanced within the EU legal framework, including discussions on EU regulations, the European Convention on Human Rights (ECHR), and Strasbourg court rulings. In particular, the next section analyses how the CFR can address political bots in conjunction with freedom of expression and information⁵⁴⁵ will be discussed considering the approach of the CJEU via closed cases remarks.

3.3.1. Political Bots and Freedom of Expression

The outputs produced by political bots raise a difficult question, which is whether they would be considered under the scope of freedom of expression and information.⁵⁴⁶ Political bots, as robots, can reach many users and content creators online in seconds. They can respond to some comments, tweets, or content even if they are automated or not automated. Moreover, the audience may seek to receive information via political bots. According to the current legal framework in the EU, the answer is negative as long as the expression originates from an AI

⁵⁴⁴ Excluding self-fulfilment from Bassini's reasons, the remaining two, which are its key role in democracy and its function in advancing the search for truth, may still be applicable to political bots. See *ibid* 5.

⁵⁴⁵ Both Article 11 of the CFR and Article 10 of the ECHR encompass a wide array of rights in their provisions. Article 11 comprises the right to hold opinions, the right to impart information and ideas, and the right to receive information and ideas. As for Article 10, the European Court of Human Rights (ECtHR) includes essentially holding the ideas, receiving opinions and imparting ideas as well as the protection of reputation, the role of media as "watchdog", protection of journalistic sources, protection of morals, specific protection for whistleblowers, specific protection for reporting on alleged irregularities by public officials. Consequently, the ECtHR adopts a broader interpretation of Article 10 of the ECHR. Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2021) 334 <<https://doi.org/10.5040/9781509933495>> accessed 10 November 2022; András Koltay, 'Freedom of Speech: The Unreachable Mirage' [2013] SSRN Electronic Journal <<https://doi.org/10.2139/ssrn.2216655>> accessed 8 December 2022; *Magyar Bizottság v Hungary, Application No 18030/11* (European Court of Human Rights); European Court of Human Rights, 'Guide on Article 10 of the European Convention on Human Rights' (2022) <https://www.echr.coe.int/documents/guide_art_10_eng.pdf>.

⁵⁴⁶ Article 11 of the CFR reads as follows: "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected." The main sources of this provision are Article 10 of the European Convention on Human Rights (ECHR), which is freedom of expression. On the other hand, United Nations (the UN) Treaties, Council of Europe Treaties, the Directives of the EU and Recommendations of the Council of Europe. Charter of Fundamental Rights of the European Union (n 39); 'European Convention on Human Rights'; Peers and others (n 545) 332 and 341.

system rather than a human actor.⁵⁴⁷ However, a human actor behind the expression, such as a programmer, would be responsible.⁵⁴⁸ Yet, the legal protection provided by the general framework remains normatively unsettled. At the current stage of technological development, the outputs or expressions produced by political bots no longer make it reasonable to search for a human actor behind them. This is because the advanced autonomy level of bots and the uncertainty surrounding the degree of human control or oversight.

As Bassini highlights, in contrast to the EU, the legal literature in the US has long engaged with this issue, and when the notion of algorithmic speech first emerged, cases addressing it in the US.⁵⁴⁹ For instance, it was debated whether search engine results could be regarded as protected speech.⁵⁵⁰ Indeed, the courts in the US have had the opportunity to test their concepts and interpretation regarding the algorithmic speech, whereas, as Bassini notes, European courts contributed less to this debate.⁵⁵¹ Yet, in the age of AI, where AI regulations are advancing rapidly at a global scale, freedom of speech has continued to be the elephant in the room, both with regard to GPAI models and AI-driven systems.⁵⁵² Furthermore, the potential for disseminating inaccurate content and disinformation has been addressed in the literature to the extent that it has entered the EU's policy agenda.

⁵⁴⁷ This negative response has previously been reflected in broader assessments of the AI Act, which argue that the Act fails to protect democratic discourse. See more Dan Taylor (n 224).

⁵⁴⁸ According to Wu, from the US perspective, the algorithmic outputs of programs consider the information from its functional perspective. For this reason, the person behind the program, namely the creator, would not hold First Amendment rights. However, if the program facilitates the users' speech, such rights could belong to the users. This article was written before the algorithmic speech had reached its advanced stage, yet the criteria of facilitating users' speech remains significant. Tim Wu, 'Machine Speech' (2013) 161 University of Pennsylvania Law Review 1506 <https://scholarship.law.upenn.edu/penn_law_review/vol161/iss6/2>.

⁵⁴⁹ Bassini (n 161) 7.

⁵⁵⁰ *Gonzalez v Google LLC* [2023] Supreme Court of the United States 21-1333; *Twitter, Inc v Taamneh* [2023] Supreme Court of the United States 21-1496.

⁵⁵¹ Bassini (n 161) 10; *Case No VI ZR 269/12* (German Federal Court of Justice).

⁵⁵² Bassini (n 161) 5.

To narrow the discussion, no comprehensive legal framework exists for political bots, despite the appearance of numerous legal tools, rather, only fragmented provisions apply. These are, in fact, different legal tools that can be applied to the various activities of bots. Political bots, as a type of chatbot, decide which users they will interact with through their algorithmic capabilities. As Sears highlights that, since fully automated production did not exist at that time, the speech protection did not need to be evaluated for bots.⁵⁵³ Yet, regarding the EU's current approach, little has changed since 2020.

Political bots can contribute information-based harms⁵⁵⁴ and can influence public opinion by boosting the popularity of diverse ideas. As freedom of expression and information in Article 11 of the CFR seems double-sided,⁵⁵⁵ there are audience's rights and speaker's rights. Article 11 provides protection for every expression (including political⁵⁵⁶) even if they are questionable, shocking, unpopular, offensive expressions.⁵⁵⁷ Accordingly, right to a forum, right to transmit, right to receive information, and right to search collectively protect political speech and political debates for speakers and audience.

The subject of freedom of speech is 'everyone', namely either citizenship nor any other legal condition is required to ensure this freedom.⁵⁵⁸ However, the ECtHR decided that corporations and enterprises can be included in 'everyone' in Article 11.⁵⁵⁹ Everyone can hold their

⁵⁵³ Alan Sears, 'Algorithmic Speech and Freedom of Expression' (2020) 53 Vanderbilt Law Review 1334 <<https://scholarship.law.vanderbilt.edu/vjtl/vol53/iss4/4>>.

⁵⁵⁴ Lamo and Calo (n 1) 1025.

⁵⁵⁵ See Peers and others (n 545) 348. Considering the multifaceted nature of Article 11, the speaker, distributor, and receiver of information must be protected equally.

⁵⁵⁶ Federal Republic of Germany v European Parliament and Council of the European Union [2000] Court of Justice of the European Union (CJEU) Case C-376/98.

⁵⁵⁷ Handyside v United Kingdom Application No 5493/72 (European Court of Human Rights).

⁵⁵⁸ While everybody has freedom of speech, only electorates can vote during the elections. However, this broad provision does not only protect the electorates' interests, also provides everyone's freedom of information during the elections. Therefore, freedom of speech draws a broader framework than rights on free elections.

⁵⁵⁹ Sunday Times v the United Kingdom (No 1), Application No 6538/74 (European Court of Human Rights).

opinions, and receive or share information and opinions freely without interference from a public authority.

Freedom of expression and information does not grant an unrestricted right to disseminate all forms of speech within its scope of protection. The limits of freedom of expression and information are drawn by States, case law,⁵⁶⁰ and now by companies.⁵⁶¹ Importantly, this protective scope excludes utterances created by machine learning algorithms.⁵⁶² Machine learning-generated content appears to have resulted in new types of content, blurring or challenging this normative grounding for certain limitations.⁵⁶³ This also emerges from the blurred line between ensuring the authenticity and neutrality of information and the risk of imposing censorship on content.

Machine learning-generated expression can be defined in the scope of Article 10 ECHR because there is no clear definition of ideas, information or opinions named in Article 10 (1).⁵⁶⁴

⁵⁶⁰ ‘Guide on Article 10 of the European Convention on Human Rights’ (n 545); ‘Freedom of Expression and Information- Explanations’ <<https://fra.europa.eu/en/eu-charter/article/11-freedom-expression-and-information#explanations>>.

⁵⁶¹ Not so long ago, former president of the United States, Donald Trump’s Facebook account was under an ‘indefinite suspension’ because of his written post and shared video regarding the attack on Capitol Hill on January 6, 2021. Then, Facebook Oversight Board decided on lifting Donald Trump’s Suspension. Ivana Vukčević, ‘Facebook Oversight Board’s Decision on the Indefinite Suspension of Donald Trump’s Account’ (2021) 12 295. See Also See Facebook Oversight Board <https://www.oversightboard.com/terms/> and the Twitter Rules <https://help.twitter.com/en/rules-and-policies/twitter-rules>.

⁵⁶² The AI-generated content can be explained as machine learning (ML)-generated content. See Katja De Vries, ‘Let the Robot Speak! AI-Generated Speech and Freedom of Expression’ in Steffen Hindelang and Andreas Moberg (eds), *YSEC Yearbook of Socio-Economic Constitutions 2021*, vol 2021 (Springer International Publishing 2022) 99 <https://doi.org/10.1007/16495_2021_38> accessed 21 November 2023.

⁵⁶³ See *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (Court of Justice of the European Union (CJEU)); ‘Opinion of Advocate General Saugmandsgaard Øe Republic of Poland v. European Parliament, Council of the European Union’.

⁵⁶⁴ There is a strong connection between Article 10, freedom of expression, of the ECHR and Article 11 of the CFR in terms of the protection area of the freedom of speech in general. The Explanations Relating to the Charter emphasise that ‘the meaning and scope of the freedom of expression and information are the same as those guaranteed by the ECHR.’ Therefore, this strong connection sets the limits of Article 11, which are also based on Article 52(3) of the CFR. The main purpose of Article 52(3) is to primarily ensure the minimum protection of the ECHR in the European Union. Article 52 includes follows: (3) In so far as this CFR contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection. It is clear about the general

Moreover, there is no clear assessment of the uniqueness or source of an expression, idea, or opinion. Rather than an issue of spreading the information, the problem can be one of the speed at which disseminated ideas or opinions are created, and the impact they can occupy in public opinion.

The ECtHR emphasises that the forms of expression can differ from new social media platforms. For instance, the forms of expression can be developed and organised by technology, namely, content can be ‘liked’ by some users which is a type of current and popular freedom of expression.⁵⁶⁵ Political bots, or bot armies, do precisely this: they aid in spreading content and increasing its visibility by automatically liking it. In fact, this activity was discussed in the *Melike/Turkey*⁵⁶⁶ case by the ECtHR, where it was identified as a form of expression. Therefore, since political bots are capable of performing in this activity, their actions also represent of a form of expression.

Freedom of information primarily includes two rights: as the provision of, or access to, information. Political bots, programmed for specific political goals, can create and spread content on digital platforms, aiming to influence public opinion. Despite their use in shaping opinions, it also is essential to protect the media pluralism⁵⁶⁷ represented by these political

framework of limitations in rights and freedoms of the Charter. Also, any limitation should be lawful, proportionate, and respect the essence of the rights or freedoms. Article 10 relies on the common values and principles in the Preamble like Article 11 belongs in the CFR. This protection extends beyond the geographical borders of the EU and is not contingent on citizenship. The inclusivity is explicitly emphasized in Article 10 which unequivocally highlights “regardless of frontiers”. Additionally, The implementation of Article 11 cannot limit the essence of the freedom of expression and information more than the limits of Article 10 of the ECHR. Consequently, the limits of Article 11 cannot be narrower than the limits of Article 10 (2) of the ECHR. See also *Al-Saadoon and Mufdhi v the United Kingdom, Application No 61498/08* (European Court of Human Rights); Peers and others (n 545) 333; European Parliament, Council of the European Union and European Commission, ‘Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02)’.

⁵⁶⁵ *Melike v Turkey* Application No 35786/19 (European Court of Human Rights).

⁵⁶⁶ *ibid.*

⁵⁶⁷ Media pluralism is a complex concept. However, the understanding point should be that this term includes all measures that ensures citizen's access to a variety of information sources, opinions, voices etc. in order for them to build their opinion without the undue influence of one dominant opinion forming power. See ‘High-Level Group on Media Freedom and Pluralism Terms of Reference’ (High-Level Group on Media Freedom and Pluralism 2011) <https://ec.europa.eu/information_society/media_taskforce/doc/pluralism/hlg/hlg_tor.pdf>.

bots. In light of the changing media environment shaped by technological advancements, the providers of information are not confined to traditional entities such as registered media houses, television channels, or newspapers. Digital media platforms are key in disseminating information, thereby allowing political bots to impact how information is presented and circulated.⁵⁶⁸

According to the ECtHR, the State must ensure that the public has access through television and radio to impartial and accurate information.⁵⁶⁹ The contention of this thesis and Chapter that similar obligations should be applicable for the social media. Hence diverse opinions and comments could influence the political perspectives during the electoral period in particular. This is why both of the courts, the ECtHR and the CJEU, support media pluralism by interpreting relevant provisions and emphasising the importance of media pluralism. However, user-generated content and citizen journalism have blurred the definitions and boundaries of traditionally recognized notions, such as media and journalism.⁵⁷⁰

In particular, the CJEU highlights in the *Buivids* case that ‘journalistic activities’ present to the public information, opinions or ideas, regardless of the platform such as newspaper, television

⁵⁶⁸ As of October 2023, the most utilised platforms for news access in EU member states vary significantly by age group. Among those aged 15-24, social media is the predominant source of news, whereas individuals aged 55 and older are the least likely to use social media for this purpose. For the older demographic, television remains the most favoured platform for news. Additionally, online press and news platforms, as well as radio, are more commonly used for news consumption than social media. In contrast, a recent study by the Pew Research Centre shows that, in the US, despite the global spread of chatbots, they have not become a regular source of news for most Americans. See Amy Watson, ‘Most Used Platforms to Access News in the Last Week in EU Member States as of October 2023, by Age Group’ <<https://www.statista.com/statistics/1399401/news-platform-access-eu-by-age/>>; Also see Michael Lipka and Kristen Eddy, ‘Relatively Few Americans Are Getting News from AI Chatbots like ChatGPT’ (*Pew Research Center*, 1 October 2025) <https://www.pewresearch.org/short-reads/2025/10/01/relatively-few-americans-are-getting-news-from-ai-chatbots-like-chatgpt/?utm_source=Pew+Research+Center&utm_campaign=e278e753fc-EMAIL_CAMPAIGN_2025_10_02_06_52&utm_medium=email&utm_term=0_3e953b9b70-e278e753fc-400659657>.

⁵⁶⁹ *Manole and Others v Moldova*, Application No 13936/02 (European Court of Human Rights) 100 and 106; *The Sunday Times v The United Kingdom*, Application no 6538/74 (European Court of Human Rights) 66.

⁵⁷⁰ *Sergejs Buivids v Datu valsts inspekcija* [2019] Court of Justice of the European Union (CJEU) Case C-345/17 53.

or digital media.⁵⁷¹ Consequently, it can be reasonable to consider that political bots can be capable of engaging in journalistic activities. For instance, bots can typically mimic real humans and may also act in ways similar to journalists. However, bots contribute to pluralism only if the term is understood as a diversity of channels, rather than a diversity of opinions and balance within content. This is because, political bots are deployed to promote specific messages as part of broader political campaign strategies. They often campaign fairly aggressively⁵⁷² and show tendency to pollute content⁵⁷³ and platforms, thus, they undermine content balance and opinion diversity. Consequently, they can stand to benefit from the diversity and protection offered by media pluralism.

Furthermore, it is essential that information remains accessible to everyone, regardless of whether it contains unpopular, unaccepted, or unwelcome speech. This is defined as a right to seek information. In particular, the right to access such information is protected by Article 11 of the CFR. However, this introduces the question: Is accuracy and impartiality a necessity for the information?⁵⁷⁴ As Bontridder and Pouillet note, the Council of the EU stated that “with regard to the importance of freedom of speech, states and administrative regulatory authorities as well as private platform providers should abstain from defining quality content or the reliability of content itself.”⁵⁷⁵

⁵⁷¹ *ibid.*

⁵⁷² Howard, Woolley and Calo (n 251) 87.

⁵⁷³ Davis and others (n 372) 1; Kyumin Lee, Brian Eoff and James Caverlee, ‘Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter’ (2011) 5 Proceedings of the International AAAI Conference on Web and Social Media 185 <<https://doi.org/10.1609/icwsm.v5i1.14106>>.

⁵⁷⁴ From the journalism perspective, the Council of Europe defines ‘information’ as the statement of fact, opinion or idea in the form of text, sound and/or picture. See ‘Recommendation No. R (2000) 7 of the Committee of Ministers to Member States on the Right of Journalists Not to Disclose Their Sources of Information’ (Council of Europe 2000) <<https://rm.coe.int/16805e2fd2>>.

⁵⁷⁵ Bontridder and Pouillet (n 385); Council of the European Union, ‘Council Conclusions on Safeguarding a Free and Pluralistic Media System’ (2020) 13260/20 para 39 <<https://data.consilium.europa.eu/doc/document/ST-13260-2020-INIT/en/pdf>>.

According to the ECtHR, politicians and public officers must be open to critics regarding their policies and behaviours, even if these critics may not be entirely precise or well-founded.⁵⁷⁶ Political bots can generate and disseminate critics that may not be thoroughly robust or completely precise during the electoral period. On the other hand, trained professional journalists⁵⁷⁷ are ethically and legally required to provide accurate, reliable, and balanced information.⁵⁷⁸ They must also adhere to the principles set by self-regulatory bodies in their country. Since the activities of political bots constitute user-generated content and can be considered within the scope of amateur journalism in the digital age, it is reasonable to expect the information provided by political bots to be accurate, especially if they act as professional journalist accounts.⁵⁷⁹

The content generated and disseminated by political bots can exploit fear or may involve racist or discriminatory elements to increase polarisation, pollute the public debate, or manipulate voters' behaviour via disinformation or misinformation. Freedom of expression and information may exclude hate speech or incitement to violence to protect tolerance and pluralism.⁵⁸⁰ Such expressions can be addressed with abuse of rights under Article 17 of the ECHR and Article 54 of the CFR. This applies to political bots as well; if political bots distribute content that is hateful or incites violence, such content is not protected under the freedom of expression. However, all content shared by bots may not contain hate, incitement

⁵⁷⁶ Balaskas v Greece, Application No 73087/17 (European Court of Human Rights)47-50.

⁵⁷⁷ Journalist is defined as 'any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication.' See 'The Status of Journalists in Europe' (Council of Europe 2018) Doc. 14505 <<https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24287&lang=en>>; 'Recommendation No. R (2000) 7 of the Committee of Ministers to Member States on the Right of Journalists Not to Disclose Their Sources of Information' (n 574).

⁵⁷⁸ Björk Eiðsdóttir v Iceland Application No 46443/09 (European Court of Human Rights)70.

⁵⁷⁹ Bots can be "necessarily detrimental to media pluralism, with curated 'newsbots' serving a media literacy and education purpose." See more 'Regulating Disinformation with Artificial Intelligence' (European Parliament 2019) STUDY Panel for the Future of Science and Technology European Science-Media Hub 3 <[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU\(2019\)624279_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf)>.

⁵⁸⁰ Peers and others (n 545) 347.

to violence, or involves discrimination,⁵⁸¹ bots can share meaningful content or vice versa causing echo chambers or supporting certain candidates or posts. Political bots, whether automatic or semi-automatic bots, execute the duties assigned by their programmers or are controlled by these same programmers.⁵⁸² In both types of political bots, since the expressions disseminated by political bots can be traced back to individuals, these expressions fall within the scope of freedom of expression. Therefore, the content political bots generate or support should be considered as expressions of the individuals who control or program them.

The EU legal framework and court approaches offer only a weak glimpse into algorithmic speech, and the current situation makes one thing clear: there is no specific regulation protecting AI-generated speech for now. A legal gap exists here. Indeed, national electoral institutions' role in combatting disinformation online seems limited from the right to freedom of expression.⁵⁸³ Additionally, after examining both the AI Act and the DSA, Bassini suggests that this gap could be addressed through more "lenient liability regime" for the AI generated outputs.⁵⁸⁴ Yet, considering the actions taken by Google and Meta to avoid TTPA requirements, both Bassini's suggestion and the strategies of big tech companies reveal the same point: neither lenient liability model nor the removal of services in specific geographic zone aligns, as big tech decides, with the aim and scope of the EU's legal framework.

⁵⁸¹ Contrary to 'the legitimate argument' which is discussed in Ethan Shattock, 'Should the ECtHR Invoke Article 17 for Disinformation Cases?' (EJIL Talk: Blog of European Journal of International Law, 26 March 2021) <https://www.ejiltalk.org/should-the-ecthr-invoke-article-17-for-disinformation-cases/?utm_source=mailpoet&utm_medium=email&utm_campaign=ejl-talk-newsletter-post-title_2>.

⁵⁸² Social media platforms generally require account registration that ties activities to an account owner, who is ultimately responsible for the actions taken by the bot. Also, Fully automated bots are initially programmed by humans. Thus, the original programming and the intended use set by the developers or the deploying organization can be traced.

⁵⁸³ Ethan Shattock, 'The Electoral Commission, Disinformation and Freedom of Expression' (2021) 71 Northern Ireland Legal Quarterly 675, 681 <<https://doi.org/10.53386/nllq.v71i4.543>>.

⁵⁸⁴ Bassini (n 161) 36.

3.3.2. Interrelation of Political Bots with Other Rights Under the CFR

3.3.2.1. Article 7 and Article 8 of the CFR

Freedom of expression and information interacts with Article 7 on private and family life and Article 8 on the protection of personal data.⁵⁸⁵ In terms of using of political bots during democratic processes, Article 39 on the right to vote and to stand as a candidate at elections to the European Parliament requires consideration in this section. Bots, by analysing data, can target certain users, manipulate them, and foster polarization by presenting various contents. In their activities, political bots may violate privacy rights and personal data protections.

Article 7 covers respect to ‘family life’ and ‘private life, home and communications.’⁵⁸⁶ The ‘communication’ is broader than ‘correspondence’ in Article 8 of the ECHR⁵⁸⁷ because it considers new communication ways thanks to technological developments. Indeed, the lack of details about communication sources or types raises notable concerns under Article 7.⁵⁸⁸ Respect for private and family life, Article 7, includes respect for the correspondence with professional and commercial content as well as correspondence between individuals. The protection of the communication includes various forms, including telephone calls, email, and internet-based communication.

Everyone has the right to keep their communications private, it remains constant despite evolving communication methods. Also, Article 7 is not restricted solely to respect for privacy; it goes beyond privacy and requires respect for communications.⁵⁸⁹ Article 8 on the protection of personal data covers processing of information about individuals.⁵⁹⁰ This is why protection

⁵⁸⁵ Charter of Fundamental Rights of the European Union (n 39) arts 7 and 8.

⁵⁸⁶ *ibid* 7.

⁵⁸⁷ ECHR regulates the ‘Right to respect for private and family life’ in Article 8.

⁵⁸⁸ Charter of Fundamental Rights of the European Union (n 39) 7.

⁵⁸⁹ *ibid* 7.

⁵⁹⁰ *ibid* 8.

of personal data is closely linked to Article 11 freedom of expression and information.⁵⁹¹ The nuance between Article 8 and Article 11 lies in their focal points; Article 8 protects individual interests by ensuring the privacy of information, whereas Article 11 primarily concentrates on the public interest in disclosing information.

Contrary to maintaining discreet communications, political bots exploit internet-based communication to identify and target accounts that may belong to various voter groups such as opposition or undecided voters. Through targeted content, these bots can silence or manipulate them. Even if political bots operate under the scope of Article 11 with the intent to disseminate information, they pre-determine several key aspects: first selection of content; second, the selection of audience; and third, frequency of dissemination. Political bots pre-determine the content of the information, i.e., the generated content they will spread, with whom they will share this information or content and how frequently they will share the information or content. This is because they engage in profiling followed by targeting users. This procedure broadly describes how political bots function.

Political bots use collected data from websites, social media platforms such as Meta and Twitter, customer support logs, or existing databases. They analyse the users' data, including geographic locations, network connections, writing tones, posting frequencies, hence, they can target users profiled based on their network or political views. The data analysed by bots can be considered personal data, as personal data encompasses all kinds of information without any restriction.⁵⁹² According to Article 22(1) of the General Data Protection Regulation (GDPR),⁵⁹³

⁵⁹¹ *ibid* 11.

⁵⁹² *Peter Nowak v Data Protection Commissioner* [2017] Court of Justice of the European Union (CJEU) C-434/1634.

⁵⁹³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016; Also see Maja Brkan, 'AI-Supported

users have a right not to be subject of this profiling and its process.⁵⁹⁴ However, it remains open how human actors would be involved in decisions made by or with help of AI systems.⁵⁹⁵ Additionally, Article 22 promise no protection for collective rights. From the perspective of political bots, even their operations produce legal effects on democratic processes, there is no remedy for collective violations.

On the other hand, when political bots analyse data that includes individuals' communication content on social media, they violate Article 7. This is because everyone has the right to keep their communications private. Second, the analysis of structured data derived from these communications could enable predictions about the user's emotional state or political views, even individuals openly sharing their communications, for example on Platform X. Additionally, even though data analysed by political bots is publicly available, it is still considered as 'personal data'.⁵⁹⁶ Moreover, even if the analysed data is publicly accessible on a digital platform,⁵⁹⁷ the data subject typically does not consent to being targeted in election processes or silenced, especially by bots that suppress opposing opinions.

Decision-Making under the General Data Protection Regulation', *Proceedings of the 16th edition of the International Conference on Artificial Intelligence and Law* (ACM 2017)

<<https://dl.acm.org/doi/10.1145/3086512.3086513>> accessed 19 October 2025.

⁵⁹⁴ Automated decision-making process includes profiling. Article 22(1) GDPR states: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Also see Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 Article 22; Similarly, Article 6(3) of the AI Act "(...)an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons." See Corrigendum to the position of the European Parliament adopted at first reading on 13 March 2024 with a view to the adoption of Regulation (EU) 2024/ of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) P9_TA(2024)0138 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)) 2024.

⁵⁹⁵ Dietrich (n 540) 2947.

⁵⁹⁶ *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2008] Court of Justice of the European Union (CJEU) C-73/07 35-37.

⁵⁹⁷ According to the ECtHR, the fact that information is already in the public domain will not necessarily remove the protection of the right to respect for private and family life, home and correspondence of the ECHR. Case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland*, Application no 931/13 (The European Court of Human Rights)134; *Volker und Markus Schecke GbR (C-92/09)*, *Hartmut Eifert (C-93/09) v Land Hessen*

Furthermore, individuals may not even be aware that their data could be used for such purposes. Namely, users may not explicitly be informed that shared data might be used for these purposes, nor may have they freely given their specific consent. However, data subjects can withdraw their consent at any time from the digital platform, but the data provided by the users can remain on the domains such as search engines. Political bots may have already processed data for which the consent is no longer valid.⁵⁹⁸ There may not be the possibility to inform the users about the period and the purpose of the potential data processing by political bots.⁵⁹⁹

The right to restriction of processing and the right to object are main bases of the data subject in the scope of the CFR and in connection with the GDPR. However, data controllers have responsibility to protect the data subject's rights. As a result, political bots exploit internet communication to manipulate voter groups through targeted messaging, often violating privacy rights under Article 7 by processing personal data without clear consent. Despite the possibility of withdrawing the consent of data subjects, data processing by bots and profiling can be an irreversible process.

3.3.2.2. Article 39 of the CFR

The EU aims to strengthen the scrutiny and the democratic accountability of European political parties and European political foundations. Besides, the Union supports fair competition between political forces by providing open, transparent and democratic legislative and electoral

References for a preliminary ruling: Verwaltungsgericht Wiesbaden - Germany [2010] Court of Justice of the European Union (CJEU) 2010 I-11063.

⁵⁹⁸ Peers and others (n 545) 267; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (n 593) Article 7(3).

⁵⁹⁹ Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) [2020] Court of Justice of the European Union (CJEU) C-61/1940.

processes.⁶⁰⁰ Political bots' activities can violate the free and secret ballot which is regulated in Article 39 of the CFR.

The right to vote and to stand as a candidate in elections in European Parliament is regulated under Article 39 of the CFR. Article 39 ensures that election of the European Parliament's members in a free and secret ballot. However, the implementation and interpretation of this right still are required by the CJEU's approach in some cases.⁶⁰¹ Since the ECtHR respects national sovereignty of the Member States, it acts cautiously when deciding on an application.⁶⁰² The right to free elections is regulated in Article 3 of Protocol No. 1 of the ECHR. It covers free elections at reasonable intervals by secret ballot. It also ensures the free expression of the opinion of the people in the choice of the legislature. The ECtHR adopts a broader perspective regarding the right to free elections compared to Article 39 of the CFR, evaluating both referendums and parliamentary elections within the scope of this right.

First, Article 39 ensures a free and secret ballot with direct suffrage in European Parliament elections. However, political bots, as mentioned above, can be able to analyse the users' political opinions before the democratic processes completed via publicly available data.⁶⁰³ The datasets provided to bots may include publicly available, but personal data, such as geo-

⁶⁰⁰ Charter of Fundamental Rights of the European Union (n 21) Preamble (33).

⁶⁰¹ *Delvigne v Commune de Lesparre Médoc and Préfet de la Gironde* [2015] Court of Justice of the European Union (CJEU) C-650/13.

⁶⁰² *Demirtaş v Turkey, Application No 14305/17* (European Court of Human Rights); *Yavaş v Turkey Application No 16576/15* (European Court of Human Rights).

⁶⁰³ Twitter offers two options to allow the public to access their data, the Streaming API(application programming interface) and the REST API (Representational State Transfer). To access any one of them, certain prerequisites have to be fulfilled. The first condition is to register a developer account. Second, this application requires a verified phone number and email address. Also, it should be described in detail how the API will be used. For instance, streaming APIs need a search term to filter the results such as 'geographical area defined by coordinates'. Schwitter Nicole and Ulf Liebe, 'Going Digital: Web Data Collection Using Twitter as an Example' (2020) <<http://policy-practice.oxfam.org.uk/publications/going-digital-web-data-collection-using-twitter-as-an-example-620948>>.

location,⁶⁰⁴ conversations, photos on social networks⁶⁰⁵ or search completed by users.⁶⁰⁶ Moreover, the votes may not remain secret because the analyses conducted by political bots can lead to various current inferences about users' political views.⁶⁰⁷ For instance, facial recognition software can predict voters' political orientation.⁶⁰⁸ Secret ballot cannot be ensured using publicly accessible data to detect users' political orientations on social networks.⁶⁰⁹ On the contrary, it poses a significant threat to the integrity of this principle, as political bots expose individuals to echo chambers or target them with specific political advertisements. In such cases, the confidentiality expected on the ballot, namely secret ballot, may already be compromised days or even months before it is cast.⁶¹⁰

Furthermore, voters may be behaviourally influenced by artificial agendas and unable to make a truly free decision. Accordingly, political bots can show content that aligns with users' political views, targeting them in this manner, which can lead to the encouraging of echo chambers. Alternatively, political bots might spread various content to polarise or influence users, potentially threatening the free ballot.

Second, individuals' free expression of the opinion of the people during the electoral process is ensured.⁶¹¹ The free expression of the opinion for both candidates and individuals should be

⁶⁰⁴ *ibid.*

⁶⁰⁵ Gianpiero Costantino, Fabio Martinelli and Daniele Sgandurra, 'Are Photos on Social Networks Really Private?' *2013 International Conference on Collaboration Technologies and Systems (CTS)* (IEEE 2013) <<https://doi.org/10.1109/CTS.2013.6567223>> accessed 6 May 2024.

⁶⁰⁶ 'User Profile Images and Banners' (X Developer Platform) <<https://developer.twitter.com/en/docs/twitter-api/v1/accounts-and-users/user-profile-images-and-banners>>.

⁶⁰⁷ According to Moore, "Personal data collection and analysis, and the ability to predict how someone will vote, subverts the secret ballot." See details Moore (n 58) 96.

⁶⁰⁸ Jakob Thrane Mainz, Jørn Sønderholm and Rasmus Uhrenfeldt, 'Artificial Intelligence and the Secret Ballot' (2024) 39 *AI & SOCIETY* 515, 518 <<https://doi.org/10.1007/s00146-022-01551-7>>; Michal Kosinski, 'Facial Recognition Technology Can Expose Political Orientation from Naturalistic Facial Images' (2021) 11 *Scientific Reports* 100 <<https://doi.org/10.1038/s41598-020-79310-1>>.

⁶⁰⁹ *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (n 596).

⁶¹⁰ Yardımcı (n 158) 61.

⁶¹¹ Article 3 of Protocol No. 1 of the ECHR only covers choice of the legislature and referendums -if they would lead to constitutional change. 'European Convention on Human Rights' (n 546) pt 3 Article 1.

protected against political bots during the democratic process. This is because political bots' activities can target supporters of candidates and may attempt to silence them. On the other hand, candidates have a right to express freely their opinions during the democratic process. Nonetheless, the potential disruptions generated by political bots on the internet, such as absurd hashtags or spam attacks, could hinder candidates from expressing themselves freely.

As a result, political bots show potential to violate individuals' right to privacy of personal political beliefs⁶¹² during democratic processes. These political bots' activities compromise the integrity of the free and secret ballot as guaranteed by Article 39 of the CFR. That is why the EU should encourage rigorous scrutiny and regulation in digital platforms to protect the fairness of elections.

3.4. Conclusion

In conclusion, the AI Act introduces a comprehensive, yet complex regulatory framework designed to classify and manage the risks associated with political bots, particularly their manipulative potential during democratic processes. While it explicitly categorises political bots as high-risk AI systems when used in electoral contexts, the Act's effectiveness is undermined by substantial ambiguities. Key among these uncertainties is the lack of clear definitions around crucial concepts such as democratic processes, elections, and referenda. Additionally, layered exceptions within the regulatory framework further complicate the practical application of the Act, potentially leaving significant loopholes.

⁶¹² Jørgen Elklit and Michael Maley, 'Why Ballot Secrecy Still Matters' (2019) 30 *Journal of Democracy* 61, 68 <<https://doi.org/10.1353/jod.2019.0042>>.

The Act's transparency obligations, while necessary, conflict fundamentally with the nature and operational purpose of political bots, which rely on their ability to convincingly mimic human behaviour. The integration of Generative AI and General Purpose AI (GPAI) models has tested the robustness of the Act, revealed structural vulnerabilities and prompted last-minute amendments to address systemic risks and fundamental rights impacts. Moreover, risk assessment processes are complicated for political bots as they may be embedded with generative-AI driven models.

Furthermore, the lack of clarity surrounding the indirect exposure of natural persons to AI-generated outputs in political campaigns creates additional regulatory uncertainty. The Act does not sufficiently clarify whether and how indirect impacts on citizens' democratic rights and freedoms should be evaluated and mitigated. Ultimately, although the AI Act represents a significant legislative step towards regulating political bots, its practical implementation faces challenges due to definitional ambiguities, complex exception structures, and conflicts between regulatory requirements and technological realities.

On the other hand, the protection of political bots' speech within the framework of fundamental rights remains unclear. One reason is that algorithmic speech, as the output of AI systems, has not been addressed in the same way as other components of AI. Another reason is that the perception that a fragmented legal framework might offer some protection ultimately proven unfounded.

Overall, this chapter examined the legal framework of political bots within EU law. In particular, it assessed how political bots are regulated under the AI Act, CFR and DSA. Accordingly, the thesis reached legal findings regarding the regulation and operation of

political bots. It also developed theoretical findings from the Chapter 2 by considering public sphere theory. However, the thesis also aims to move beyond theoretical and legal analysis. Therefore, Chapter 4 presents a thematic empirical study based on interviews conducted with AI professionals. The following chapter explores how AI systems, bots, political bots, and democratic processes are perceived and understood in practice. In this way, the research combines theoretical and legal frameworks with practical insights and further develops the policy recommendations presented at the conclusion of the thesis.

Chapter 4: Analysis of Interview Data

4.1. Overview

This chapter provides empirical findings derived from interview data. However, the data and findings presented in Chapter 4 are not designed to test, verify, or falsify the arguments developed in Chapters 2 and 3 in the manner of a traditional social science hypothesis-testing framework. Rather, the interview data are intended to complement and add to the conceptual and legal insights developed in those chapters.

This chapter provides the findings from a thematic analysis based on anonymised interview data. The data were transformed into the MAXQDA software and analysed in line with the methodology outlined in Chapter 1 Section 1.2. The purpose of this research is to explore whether political bots are regulated under the AI Act, and if so, to what extent, from a legal perspective. If a regulatory gap is identified in the Act, the thesis aims to provide practical recommendations to address this gap, drawing on the findings from interviews conducted with professionals in AI. Thus, extensive insights into whether and how the necessity and adequacy of regulating political bots were gathered from interviews conducted with professionals in AI across Europe. In the analysis, to ensure the clarity, figures are used to visualise findings. Anonymised quotes from the interviewees are included to explain the findings and demonstrate how they were substantiated.

This chapter consists of two main sections. The first section details the thematic analysis of interview data completed using MAXQDA. It explains: themes that are used for the analysis; why they were chosen; and how they are supported by data from the interviews. The findings

related to themes are discussed at the end of the first section. The second section considers the value of the research, implications for practice, and recommendations for future research.

4.2. Interviewing Process

4.2.1. Interviewing

15 interviews with professionals in AI have been conducted as a part of this research. At the beginning of interviews, all participants are asked a common set of open-ended questions. These questions aim to explore how interviewees reflect on their demographic backgrounds. Also, each interviewee is informed about the purpose of this common section questions. The interviews involve professionals in AI from three subgroups: public sector professionals, company professionals, and NGO representatives. This classification for the subgroups was necessary to clarify the structure of the research. However, these classifications remain permeable when professional experiences of participants are reviewed. Therefore, participants provide insights informed by diverse perspectives and professional contexts thanks to their cross-sectoral experience. As a result, their responses to interview questions reflect multifaceted and process-oriented understandings of regulatory developments in technology.

The research utilizes eight specific research questions tailored to each subgroup in order to better understand their distinct approaches. The findings are evaluated based on both the commonalities across different subgroups, and the overall conclusions drawn from the interviews. Additionally, the analysis of responses to open-ended questions is analysed using the MAXQDA software, and employing a thematic analysis approach. Thus, research findings are derived from the analysis conducted using MAXQDA software on the gathered data.

This software program provides analysis of qualitative data.⁶¹³ Various data types and formats, including surveys, video and audio recordings, interview transcripts, research reports, articles, journals, and bibliographic data, can be analysed using MAXQDA. Since the analytical technique of qualitative data segmentation plays an important role in conducting qualitative analysis, MAXQDA provides several core functions for qualitative data analysis, including coding, text search, automatic coding, paraphrasing, inserting memos and comments, and code retrieval, all facilitated through its software capabilities.⁶¹⁴

MAXQDA effectively supports thematic analysis,⁶¹⁵ which is flexible, widely used in many disciplines, and aims at a detailed description of data. This is why 15 conducted interviews have been analysed using this software, MAXQDA, for thematic analysis. Although the qualitative research is criticised for lacking rigour because of its relatively small sample size and limited scope, this research accepts that the concept of layering can effectively address such concerns. In qualitative research, what is important is both the profile of the respondents and the relevance of their profiles to the research questions, if interviews are selected as method. In this study, participants were invited only after their backgrounds (professional and academic) had been examined in detail. Interviews were subsequently conducted with those who agreed to participate. In this research, the repetition of similar themes across the data, such as lobbying, power asymmetry, media environment, political communication, face-to-face communication reflects the continuity, strength, and authenticity.⁶¹⁶

⁶¹³ Kuckartz and Rädiker (n 180) 1.

⁶¹⁴ *ibid* 5.

⁶¹⁵ Ann Lewins and Christina Silver, *Using Software in Qualitative Research: A Step-by-Step Guide* (2. ed, SAGE 2014) 68.

⁶¹⁶ Samantha McAleese and Jennifer Kilty, 'Stories Matter: Reaffirming the Value of Qualitative Research' [2019] *The Qualitative Report* 836 <<https://doi.org/10.46743/2160-3715/2019.3713>> accessed 6 October 2025.

Furthermore, qualitative studies are not designed to present statistical generalisability.⁶¹⁷ Therefore, expanding the sample size may provide a more cumbersome dataset.⁶¹⁸ The sample size should be guided by the research questions, well-designed interviews questions and analytical requirements such as data saturation, the depth and relevance of participants' contributions, their characteristics, and their willingness to answer the research questions. In this research, fifteen interviews were conducted. The findings do not rely on generalised insights, but rather on analysing how participants approached the open-ended questions and how they examined their own relationships with AI. For this purpose, qualitative data analysis was conducted by utilising the software, MAXQDA, to assist in identifying and organising thematic patterns within the data.

While in most qualitative research the analysis begins concurrently with data collection, as the emerging data shape ongoing interviews and data collection.⁶¹⁹ For this purpose, the use of MAXQDA supports the qualitative analysis process by facilitating systematic coding. The codes are key tools of MAXQDA. Accordingly, the data obtained from interviews has been systematically analysed and organized via codes. The software also assigns meaning to the gathered data material from AI experts through interviews, structuring it into text segments. The software, MAXQDA, also facilitates assigning meaning to the data material collected from AI experts through interviews, and structuring it into text segments. The list of the codes used during the analysis in this research project is provided as Appendix 1 to the thesis.

Qualitative data is generally not concerned with the quantification of data.⁶²⁰ Nevertheless, in this thesis, MAXQDA enabled to present several visual figures derived from the codes. These

⁶¹⁷ C Pope, 'Qualitative Research in Health Care: Analysing Qualitative Data' (2000) 320 BMJ 114, 114.

⁶¹⁸ *ibid.*

⁶¹⁹ *ibid.*

⁶²⁰ *ibid.*

visual figures were based on the codes used in the analysis and the on the frequency of participants' word choices during responding the questions. The figures were included in the study to illustrate meaningful patterns within the data.

On the other hand, while computer software may assist in organising, managing, and reconfiguring data, and even in detecting anomalies or exceptions, it cannot perceive theoretical connections or determine the structure for analysis.⁶²¹ For this reason, the qualitative analysis depends on the researcher's own analytical skills. At this point, the researcher takes the analysis beyond a basic descriptive and asserts hypotheses or propositions about the data.⁶²²

To analyse the data, the first step was the anonymisation of data as part of the research data preparation. In this process, names and any identifiable details of the participants were anonymised in the interview text. Then, the text was converted into a line numbered text format, facilitating the use of quotations when presenting the findings. In a good qualitative analysis, the research claims to reflect some of the truth of a phenomenon by reference to systematically gathered data. For this purpose in Chapter 4, brief anecdotes are used exclusively to illustrate participants' perspectives as they emerged within their lived contexts, rather than as standalone or subjective narratives. The research avoids becoming unreflective and descriptive; in contrast, it is focused on a coherent line of inquiry.

⁶²¹ *ibid* 116.

⁶²² *ibid*.

4.2.2. Demographic Reflections on Interviews

This section introduces the interviewees who attended the research and shared insights. The purpose of the section is to provide the demographic reflections regarding the interviewees. The section introduces also initial findings of the interviews which were conducted for this research project. There are three reasons for conducting a demographic reflections of interviews via gathered data. The first reason is to provide transparency regarding the profile of interviewees. Second, the analysis demonstrates whether the findings of the interviews, in Chapter 4, offer insights relevant to a broader population that would contribute to a better understanding of the scope and relevance of the findings. Finally, demographic reflections of gathered data helps to clarify the research.

The demographic composition of the interviewees can be summarized with gender, educational background, and the sectors in which they have gained professional experience, such as the public sector, the private sector, or within NGOs.⁶²³ This reflection further demonstrates the motivations of interviewees to follow developments in technology regulation. For instance, educational background or professional experience were reflected to demonstrate participants are professionals in AI field. The interviews were conducted with professionals in AI across the Europe. The interviewees attended this research from Sweden (1), Italy (2), Ireland (4), Netherlands(2), Belgium(3), Austria (1), Greece(1), and Latvia(1).

For instance, SG1 comprises interviewees who held positions in the public sector at the time of interviews. This subgroup covers participants from academics in EU universities, rapporteurs in the European Commission, and politicians in parliaments. Accordingly, their roles in relation to AI involve directly participating in AI rulemaking processes, providing

⁶²³ The reasons for dividing subgroups are explained above in the Section 4.5.3.2. Interviewing.

reports and briefings to representatives and the European Commission, and contributing opinions and expertise throughout these regulatory processes. All of those in SG1 hold a master's degree, at least. For three participants, the motivation to follow developments in technology regulations was directly linked to their professional roles. For one participant, personal motivation⁶²⁴ sparked their engagement with these developments, whereas another cited concern about broader societal transformation as their primary motivation. An overview of SG1 is provided in Figure 3.

SG1	Gender		Educational Background			Interest in Tech Regulation		
Participants	Women	Men	Bachelor's Degree	Master	PhD	Professional Responsibilities	Personal Motivation	Societal Concerns
5	3	2	0	5	0	3	1	1

Figure 1. Overview of SG1.

SG2 includes interviewees who worked for NGOs during the interview period. In SG2, participants included individuals working in NGOs based in the Netherlands, Ireland, and Belgium. Their NGOs focus on human rights and fundamental rights and freedoms, particularly the protection of freedom of expression and information in the EU, as well as digital rights, media independence, and democratic protections. So, their roles in relation to AI involved monitoring regulatory developments in AI, following the policies of technology companies, and focusing on governmental strategies at both national and international levels. All held postgraduate degrees, with one interviewee holding a PhD (See Figure 4). All participants

⁶²⁴ The research consider non-professional interest during the interview analysis, as public perceptions, informal engagement, and individual awareness may still shape understandings of bot, political bots and democratic processes beyond formal professional expertise. This category can be called as personal motivation in this research.

stated that their engagement with developments of technology regulations was due to their professional responsibilities. This means participants highlighted that they were interested in topic primarily because of their professional responsibilities. They stated that they would not otherwise engage with this topic in their daily lives.

SG2	Gender		Educational Background			Interest in Tech Regulation		
Participants	Women	Men	Bachelor's Degree	Master	PhD	Professional Responsibilities	Personal Interest	Societal Concerns
5	3	2	0	4	1	5	0	0

Figure 2 : Overview of SG2.

SG3 includes participants from the private sector. In this subgroup, all participants were working for companies. In SG3, participants were working in companies based in, or with branches located in, Latvia, Austria, Ireland, and Sweden, operating across the EU at both national and multinational levels. Accordingly, two participants were working in the management consulting field. These participants shared the insights from the perspective of their global analytics and advisory firm which measures public opinion for democratic processes. Additionally, two participants were working as Chief Executive Officers in companies involved in conducting political campaigns, increasing candidate visibility, and providing advice on political campaign strategies. SG3, a participant was also working as Chief Executive Officer in a firm specialising in fine-tuning LLMs. The company was developing machine learning classification systems for the media, insurance, and legal technology sectors. Also it involved in designing systems to counter potentially defamatory and harmful content. As a result, these companies either offered consultancy services for political campaigns or

provided content moderation on social media. The descriptions of their work are included below to illustrate which aspects of the private sector are reflected in their insights.

Interviewee 1 described their work as “*paid social ads*” (SG3-Interview 1, Pos. 75). However, most of what they do is the analysis of candidates’ social media accounts and giving advice, for instance, “*What is working on your page? What are our recommendations would be to improve your content for the algorithm?*” (SG3-Interview 1, Pos. 75). They also analyse political opponents’ pages to see what is working, providing a kind of “*soft analysis of content*” (SG3-Interview 1, Pos. 75). In addition, they do some “*programmatic ad buying as well as social.*” (SG3-Interview 1, Pos. 75)

Interviewee 2 explained that their company provides opinion polls before and after elections. However, they highlighted: “*We strictly only do analysis.*” (SG3-Interview 2, Pos. 105, 107). Interviewee 3 mentioned that their work focuses exclusively on identifying risky content and providing content moderation support. Political campaigns are included within this scope (SG3-Interview 3, Pos. 157-158).

Interviewee 5 said their work is not about testing social media campaigns, but rather about testing material that goes into traditional media, because that is where the “real reach” lies (SG3-Interview 5, Pos. 100). They also emphasised that their main activities are political polling and market research (SG3-Interview 5, Pos. 97).

Among the five interviewees, three held a master’s degree and two held a bachelor’s degree. Regarding their motivation for following developments about technology regulations, three participants referred to professional responsibilities, one cited both professional responsibilities and societal concerns, and one mentioned personal interest alongside professional interest.

SG3	Gender		Educational Background			Interest in Tech Regulation		
Participants	Women	Men	Bachelor's Degree	Master	PhD	Professional Responsibilities	Personal Interest	Societal Concerns
5	1	4	2	3	0	3	1	1

Figure 3 : Overview of SG3.

Overall, the majority of participants explained their interest in technology and tech regulations as being related to their professional responsibilities. The conducted interviews also ensured gender balance among the participants. On the other hand, professional background of the participants is summarised in Figure 6. This distinction between subgroups reflect participants' current institutional affiliations. However, the interviews and publicly open career information of the participants indicated that some participants had experience across multiple sectors. For example, one participant currently working in the public sector had previously worked in the private sector. As shown in the Figure 6, only two participants have experience across all three sectors (Subgroup 1, Interviewee 4 and Subgroup 2 Interviewee 4).

		Private Sector Experience	Public Sector Experience	NGOs Experience
Subgroup 1 (SG1) (Public Sector)	Interviewee 1	X	X	
	Interviewee 2		X	
	Interviewee 3		X	X
	Interviewee 4	X	X	X
	Interviewee 5	X	X	
Subgroup 2 (SG2) (NGO Sector)	Interviewee 1			X
	Interviewee 2		X	X
	Interviewee 3	X		X
	Interviewee 4	X	X	X
	Interviewee 5		X	X
Subgroup 3 (SG3) (Private Sector)	Interviewee 1	X		X
	Interviewee 2	X		
	Interviewee 3	X		
	Interviewee 4	X		
	Interviewee 5	X		
3 Subgroups	15 Interviewees	10 Interviewees have private sector experience.	8 Interviewees have public sector experience.	8 Interviewees have experience in NGOs.

Figure 4. Experience of interviewees.

4.2.3. Transcription

Transcription is an essential step before the analysis of interviews because it signifies the point when raw data begins to transform into an analytical form. Additionally, this process can be thought of as an initial analysis because converting verbal conversations into a written format structures the discourse and provides more systemic examination.⁶²⁵ On the other hand, detailed transcripts can be used as evidence for research findings.⁶²⁶ However, the qualitative data are not necessarily small scale, as the transcription of a single interview can require several hours and result in 20–40 pages of detailed text.⁶²⁷

⁶²⁵ Svend Brinkmann and Steinar Kvale, *Doing Interviews* (Uwe Flick ed, Second edition, SAGE 2018) 108.

⁶²⁶ Tim Rapley, *Doing Conversation, Discourse and Document Analysis* (2nd edition, SAGE 2018) 54.

⁶²⁷ Pope (n 617) 114.

Therefore, after each interview, transcription was conducted using a computer and headphones. Verbatim transcription of an hour-long interview may require at least six to eight hours.⁶²⁸ For this research, the interviews lasted between 45 minutes to an hour. AI-driven online tools for transcription were not used considering data privacy policies of Maynooth University. As a result, interviews were manually transcribed to ensure the privacy of participants, and the data were anonymised immediately as part of the transcription process.

Also, there are two approaches for transcribing interviews: naturalism and denaturalism.⁶²⁹ This research adopts a denaturalist approach and any distinctive sounds, and vocalisations such as “umm” and “err” are removed.⁶³⁰ To provide reliability of transcripts, the records of interviews were listened to twice before any data was removed securely. To ensure validity of transcripts, the transcription process focuses on the meaning and context of the conversation for analytical use.⁶³¹ The main codes defined for this analysis include interviewees' perspectives on political bots, democracy, AI definitions, ethics, EU law, the AI Act, media, and media blackout periods. The list of codes is presented in Annex 3 of the thesis.

4.3. Ethical Considerations

4.3.1 Ethical Approval

Prior to commencing the study, ethical approval was sought via the Social Research Ethics Sub-Committee (Annex II). Furthermore, the proposed research was discussed with and agreed by the School of Law and Criminology of Maynooth University where I am registered as a

⁶²⁸ Rapley (n 626) 57.

⁶²⁹ See more DG Oliver, JM Serovich and TL Mason, ‘Constraints and Opportunities with Interview Transcription: Towards Reflection in Qualitative Research’ (2005) 84 *Social Forces* 1273 <<https://doi.org/10.1353/sof.2006.0023>>.

⁶³⁰ According to this approach, naturalism describes the practice whereby every verbal and non-verbal expression is transcribed in fine detail. *ibid*.

⁶³¹ Brinkmann and Kvale (n 625) 112.

PhD student. The research complied with the Maynooth University Research Ethics Policy,⁶³² Maynooth University Research Integrity Policy,⁶³³ and Maynooth University Data Protection Policy.⁶³⁴

This research has no access to confidential business information, confidential government policies or strategies, and confidential financial information of NGOs during any aspect of this study. The funding for this study is from the Research Ireland and the ADVANCE CRT, and is not connected in any way to political parties or any political figures. The research and the researcher align with the Maynooth University Conflict of Interest Policy.⁶³⁵

4.3.2 Confidentiality and Anonymity

Researchers are responsible to ensure that participants understand the extent of anonymity and confidentiality. This responsibility is offered at all stages of the research from data gathering to dissemination.⁶³⁶ Participants have a right to privacy and anonymity and are made aware of this entitlement.

The collected data via interviews is stored in a secure and accessible form.⁶³⁷ Additionally, all interview data is stored in an encrypted format. All information related to the identification of an interviewee or a person, directly or indirectly, such as names, locations, company names, or specific to social, cultural, economic, genetic, or mental identity of a person has been

⁶³² 'Maynooth University Research Ethics Policy (Version: 2)'.

⁶³³ Research Committee, 'Maynooth University Research Integrity Policy'.

⁶³⁴ 'Data Protection Policy'.

⁶³⁵ 'Research and Commercialisation Conflict of Interest: Policy and Guidelines (Revised:2019)'.

⁶³⁶ 'Maynooth University Research Ethics Policy (Version: 2)' (n 632) 13.

⁶³⁷ *ibid* 14.

removed.⁶³⁸ The context of anonymity and its limits were made aware to all participants as written in the Interview Information Sheet of the research.

4.3.3 Informed Consent

Miller and Boulton describe informed consent as a concept that articulates the ethical relationship, namely appropriate relationship, between researcher and research participant.⁶³⁹ For valid consent, participants decide to attend the research voluntarily.⁶⁴⁰ Free and informed consent of participants would be considered as ethical standard of the social research.⁶⁴¹ Accordingly, the informed consent would outline clearly the details about what engagement in the research includes.⁶⁴² Consistent with Klykken, this research views knowledge as a continuous and collaborative process rather than a static and individualised product.⁶⁴³ Therefore, consent is regarded as a dynamic process that participants may withdraw from at any time.

Researchers ensure that all potential participants understand what is involved in a study. In this research, the informed consent is obtained with the utmost attention.⁶⁴⁴ Participants' voluntary informed consent was obtained at the start of each interview. According to MU Research Ethics Policy, informed consent needs to be recorded, but a written version of form is not strictly required.⁶⁴⁵ The informed consent is received after potential participants are informed about all aspects of research process.

⁶³⁸ 'Data Protection Policy' (n 340).

⁶³⁹ Tina Miller and Mary Boulton, 'Changing Constructions of Informed Consent: Qualitative Research and Complex Social Worlds' (2007) 65 *Social Science & Medicine* 2199, 2199 <<https://doi.org/10.1016/j.socscimed.2007.08.009>>.

⁶⁴⁰ Fride Haram Klykken, 'Implementing Continuous Consent in Qualitative Research' (2022) 22 *Qualitative Research* 795 <<https://doi.org/10.1177/14687941211014366>>.

⁶⁴¹ *ibid* 795.

⁶⁴² Klykken (n 640).

⁶⁴³ *ibid* 797.

⁶⁴⁴ 'Maynooth University Research Ethics Policy (Version: 2)' (n 632) 14.

⁶⁴⁵ *ibid*.

Accordingly, the interviewees are informed about the content of this study as per the guidelines of Maynooth University Ethics Policy. Each participant in this research is informed by presenting “Interview Information Sheet”. This document, Interview Information Sheet, is approved by Social Research Ethics Sub-Committee as well.

The participants who are professionals working in this field, are informed of what the findings of this research are used. They are also informed about the research project, briefly informed on utilization of software robots during political elections, mentioning supervisors of this project, funding details of the project, main goals of research. Additionally, it is acknowledged that follow-up questions may arise, and the researcher is willing to answer these queries through email communication. Moreover, Maynooth University and supervisors of this research are available to provide additional information or guidance as needed.

4.4. Data Analysis

This section outlines the data analysis process conducted in this research. For this research, a number of phases are undertaken. Initially, potential interviewees have been approached using professional tools such as institutional email address or official web contacts. Following this, interviews are scheduled at a mutually convenient time for both the potential interviewees and the researcher. The interviews are conducted in-person or online depending on the interviewees’ schedules.

Before starting the interview, the potential interviewees are reminded of the ‘Information Sheet’ briefly. In particular, the purpose and scope of the research, data protection, and interviewees’ right to withdraw from the interview at any time are reminded. Subsequently, the

interview can be recorded with the explicit and informed consent of the interviewees. After the interviews, the transcription process is completed. These transcriptions are categorised, repeatedly reviewed, and codes are extracted from them for use in MAXQDA. Additionally, memo writing, coding, and renaming codes are parts of these analytical process.

4.4.1 Data Analysis Software

MAXQDA assists in organising interview data and streamlines various analytical processes, including coding, memo writing, and categorization. It enables data comparison for this research among sub-groups. Accordingly, anonymised interview transcripts first upload to the system. These transcripts are then organised into three separate folders corresponding to the sub-groups that have been determined at the outset of the research. Each transcript is placed in the relevant folder based on its content. Subsequently, an initial reading of the uploaded documents is conducted. The purpose of this preliminary reading is to develop an understanding of the potential codes, which are the concepts that would later form the foundation of the thematic analysis.

During this stage, notes are taken regarding possible codes, and relevant sections of the transcripts are highlighted. The second and third rounds of reading primarily focus on coding and recording the emerging codes. To assess the suitability, quality, and relevance of the preliminary codes for analysis, the transcripts are revisited several times. During this process, additional codes are considered for incorporation based on insights drawn from both the interviews and the ongoing analytical process.

Thus, this software allows for code creation, memo writing, highlighting text passages with assorted colours, searching text, and also provides visualisation of the most frequently used

words in the text.⁶⁴⁶ Document system and code system of the data are presented in Annex VI and Annex VII.

4.4.2 Coding and Memos

MAXQDA software provides various tools for keeping memos such as project memos, free memos, document memos, and code memos.⁶⁴⁷ The project memos which are used to describe the entire project are used for this research via MAXQDA.⁶⁴⁸ Project memos, providing a summary of methodological procedure, is saved into the document during the project preparation and imported data to MAXQDA software. For this research, project memos are presented in Annex IX. Also, code memo and free memo are used for analysing interviews. Code memos are extracted from interviews and used for categorising definitions, in particular AI and bot definitions of participants. Free memos are also used to categorise common themes to reflect the general tendencies of subgroups to which the interviewees belong. By using word cloud, a list of word frequencies are generated via Voyant Tool and MAXQDA are presented in section 4.6., specifically to reflect the textual themes used by interviewees in their definitions.

The reason for using the Voyant tool in this research was to obtain an early visual representation related to participants' definitions of AI, before the analysis of all interview transcripts had been completed. For this purpose, the words most frequently used by participants, along with the insights they provided, were analysed and uploaded to the Voyant tool, which generated the corresponding visual output.

⁶⁴⁶ Kuckartz and Rädiker (n 180).

⁶⁴⁷ *ibid* 285.

⁶⁴⁸ *ibid* 52.

This visualization are presented in section 4.6., Figure 7, Figure 8, and Figure 9. At that stage, it was not possible to create a similar visual output using MAXQDA, as the analysis had not yet been fully completed. However, once the entire analysis and the review of all interview transcripts were finalised, a word cloud illustrating the most frequently used terms was also generated using MAXQDA, which is likewise presented in section 4.6., Figure 1.

For the qualitative content analysis, categories are used to organise interview data, classify different types of responses or themes and analyse statements. This research conduct thematic analysis by using the data which is collected using semi-structured interviews. As thematic analysis is a flexible method and focuses on the detailed description of data, the research project leverages this advantage.⁶⁴⁹

For this research, interviews are analysed by developing thematic categories that point out thematic areas and structure the content. Thematic analysis takes shape in parallel with the review of transcribed interviews. During this process, the codes to be used for this analysis are generated. The coding process requires asking analytical questions on gathered data by the researcher, thereby further understanding of the studied phenomenon can be presented. Categories may include simple words or can be a short phrase that summarize the analysed content. The hierarchical coding category system is used for this analysis.

4.5. Research Integrity, Trustworthiness and Limitations

Qualitative research is often criticised because of its limited ability to provide objective findings. Also, the findings may not be consistently replicated, raising concerns about reliability of the research. In order to ensure trustworthiness, this research benefited from

⁶⁴⁹ *ibid* 7.

MAXQDA software, and four principles of validity of qualitative research: sensitivity to context, commitment and rigour coherence, transparency, impact and importance.⁶⁵⁰

Accordingly, sensitivity of context refers to the process of becoming familiar with the research area.⁶⁵¹ Thus, a researcher becomes sensitive to the sociocultural context of the participants throughout the research process. In order to address this principle, prior studies are examined, and institutional documents related to interviewees' professional environments are considered. This preparation helps refine semi-structured and open-ended interview questions, and also helps to shape potential follow-up inquiries for interviewees. The preparation ensures contextual sensitivity.

In line with this principle, Yardley states that exploration and analysis need to provide deeper insights.⁶⁵² To ensure commitment and rigour, the researcher ensures that approached professionals relevant to study's context, so that the collected data remains meaningful and applicable to the research. During this process, informed consent was obtained from all participants.

The principle of informed consent formalises participants' contribution to the research and helps to establish a research relationship based on trust and integrity for the research. For this reason, participants were fully informed and reminded that they had complete freedom to decide whether or not to take part in the research.⁶⁵³ In doing so, this research demonstrates its

⁶⁵⁰ Lucy Yardley, 'Demonstrating the Validity of Qualitative Research' (2017) 12 *The Journal of Positive Psychology* 295 <<https://doi.org/10.1080/17439760.2016.1262624>>.

⁶⁵¹ Sinead Walker, 'A Constructivist Grounded Theory of the Influences and Practices That Are Thought to Promote a Sense of Belonging in a Primary School Context' (University of Essex 2019) 70.

⁶⁵² Yardley Lucy, 'Demonstrating Validity in Qualitative Psychology' in Jonathan A Smith (ed), *Qualitative Psychology: A Practical Guide to Research Methods* (SAGE Publications 2008).

⁶⁵³ Klykken (n 640) 795.

commitment to ethical integrity and the trustworthiness of both the data and the overall research process.

For this purpose, the research utilizes MAXQDA software to keep detailed records for reporting the findings and assessing the quality and reliability of data collection.⁶⁵⁴ In particular, the research benefits from document memos via MAXQDA,⁶⁵⁵ through which information about the context of the interview can be presented in a more reliable manner.

Coherence refers to the degree to which the study maintains logical consistency and presents a well-structured, integrated framework. Despite the complexities of coherence in interdisciplinary research, this research adopts thematic analysis as a key methodological approach to derive its findings. Additionally, Chapter 4 of this thesis integrates the research outcomes and findings, presenting recommendations and policies for future studies. Therefore, it provokes further thought and discussion with regard to regulation of political bots in the EU framework. It will be significant in terms of democracy culture of society. As a result, this research has direct and practical implications.

4.5.1 Research Design and Limitations

This research sought to explore the legal framework of political bots within the AI Act. For this purpose, a socio-legal research approach was adopted, and the views and experiences of professionals in AI were sought through semi-structured interviews. Adopting the semi-structured interviews as a method of this socio-legal research offered breadth and depth of insight. This method and research approach were adopted as part of the qualitative research

⁶⁵⁴ Michael C Gizzi and Stefan Rädiker (eds), *The Practice of Qualitative Data Analysis* (MAXQDA Press 2021) 37 <<https://doi.org/10.36192/978-3-948768058>> accessed 4 March 2025.

⁶⁵⁵ *ibid.*

methodology. It enabled understanding of legal gaps and societal concerns from a professional perspective regarding political bots, particularly in relation to freedom of expression and information. A socio-legal research approach using semi-structured interviews was therefore considered an appropriate method to employ.

However, some of the limitations of this research are a consequence of the research design. A frequent criticism of qualitative research methodology is that it is difficult to reach a generalisable conclusion based on limited interviewees, and open-ended questions in the interview design.⁶⁵⁶ However, the intention was not provide generalisable findings at this level as it acknowledged that each country has a unique electoral system. Instead, societal concerns are highlighted by the findings, and the research concludes with recommendations for addressing legal gaps related to these concerns. Thus, the analysis promotes to what extent this research may or may not be applicable beyond the specific context within which the data was gathered.⁶⁵⁷

On the other hand, the number of interviewees in this research can be considered small, especially in relation to the broader population of professionals in AI. Thus, a larger and more diverse range of participants would have strengthened the findings of this research. The reason for not seeking a larger and more diverse range of participants was that the AI Act was still a relatively new attempt to regulate AI systems at the time of planning the interviews. One hesitation was whether there would be a sufficient number of professionals in the three relevant areas, namely, Subgroups 1, 2, and 3. Another concern was the willingness of potential participants to engage in a discussion on this topic. In particular, reaching participants from

⁶⁵⁶ According to Willig, objectivity or absence of bias are not considered as meaningful criteria for addressing ‘good’ qualitative research. Considering this view, this section does not engage with critiques based on potential discussion of objective or unbiased research methodology. Carla Willig, *Introducing Qualitative Research in Psychology: Adventures in Theory and Method* (Second ed, Open university press 2008) 150.

⁶⁵⁷ *ibid* 151.

SG3 was challenging, as many of them were bound by confidentiality agreements with their current or former employers. These concerns contributed to the decision to keep the number of interviews limited.

However, multiple perspectives were obtained and rich, insightful, and professional perspectives of participants were gathered during the interviews. This increases the credibility of the current research. Additionally, the process of approaching potential interviewees also poses a limitation for this research. potential interviewees were approached thorough official communication channels, such as official website, official email address, etc. However, some of these communication efforts remained unanswered.

Nevertheless, each potential interviewee was informed about the research, the data collection process, the significance of their participation and the ethical principles guiding the study. They were also provided with the details on how the interview data would be stored and used. Additionally, interviewees were informed of their rights to withdrawn from the study at any time. The written, detailed and ascertain consent from interviewees was obtained for the participation in the interview of this research. Therefore, there was no risk that selection bias occurred because the participants expressed their willingness to take part in the research.

During the process of approaching potential interviewees, participants working in public sector and NGOs were generally responsive, which allowed to conduct interviews smoothly. However, significant challenges had to be overcome to reach potential interviewees in the private sectors, particularly professionals from big tech companies. For this purpose, official and professional communication channels were used, and even efforts were also made through a snowball method to reach professionals from big tech companies. However, these attempts remained limited. One of the main reasons for this limitation may be the confidentiality agreements.

However, it was assumed that conducting this research near Dublin, where various tech companies have their branches or headquarters, would facilitate to reach potential interviewees. As a result, the interviews conducted with the private sector subgroup focused on professionals from smaller companies and well-established political consultancies. These interviews provided valuable and unique insights that enriched the research.

As discussed in chapter four, interview questions were designed for three different subgroups. However, interview questions explored how interviewees reflect on their demographic backgrounds. Also, the interviews captured the general understanding of AI and political bots from the participants. The questions in the common section were posed for every interviewee. Sector-specific questions were directed to each subgroup to explore differences between sectors and understand the distinct perspectives of the interviewees on the AI Act process and related themes on it.

4.5.2. Trustworthiness

A frequent criticism regarding qualitative research is the possibility of researcher bias, as the analysis may rely on subjective interpretation. However, this research provides relevant charts and coded details generated by MAXQDA software to support the thematic analysis. On the other hand, each stage of the research and analysis process were detailed explained during the ethical approval application procedure to avoid the potential risk of researcher bias. The researcher was fully aware of this risk and consider relevant steps to mitigate it. Accordingly, the researcher avoided leading the interviewees at no stage. Instead, the interviewees were asked open-ended questions, which are included in Annex 5, Annex 6 and Annex 7 of this thesis.⁶⁵⁸ Thanks to this approach, the analysis were prevented against biased interpretation,

⁶⁵⁸ Further details on this can be found in Chapter 4, section 4.7, titled Integrity and Trustworthiness.

thus, it is ensured that the findings and conclusions were presented objectively. Additionally, the anonymised quotations from the interviewees were included to support the findings, enhance credibility and to avoid equivocal evidence.

4.5.3. Research Implications

The research reflects the understanding of the legal framework for regulating political bots without interfering with the freedom of expression and information. This contribution is pertinent and timely for various reasons. First, there are ongoing attempts to regulate AI systems around the world. Second, the multilayered regulation efforts for AI systems are shaped by currently complex and vague legislation. Third, AI-driven technologies pose risks that may increase vulnerability of democracy.

As discussed in Chapter 2, there is research in the literature which indicates how political bots impact political elections. This project extends this research area into the regulatory framework by providing a qualitative exploration of how political bots are regulated in the AI Act. A qualitative research methodology and semi-structured interviews were adopted to explore the perspectives and practices of professionals in AI. Accordingly, the data could be collected at a critical time, prior to the final path of the AI Act and during the global elections year in 2024. Therefore, the research offers timely insights, informed both by the dynamics of the 2024 elections and by the evolving framework of the AI Act.

4.6. Theme Development for MAXQDA Analysis

As detailed in section 1.2.2. the research questions for this study were:

RQ1: How are political bots used as tools for manipulation in political elections in Europe?

RQ2: How could the European Union's AI Act prevent political bots from being used as a tool for manipulation without interfering with pluralism and freedom of expression and information?

In response to these research questions, the themes used in the analysis help to understand how political bots are perceived by professionals in AI from different sectors of society and identify legal gaps and challenges to develop policies. The themes of the research were identified through a combination of continuous review, theoretical analysis, and iterative engagement with the interview data. While designing the interview questions, several potential themes were initially identified based on the literature review and the development of the theoretical framework of the research, such as democracy, governance, and bots. Following the completion of all interviews, the main themes were designed as AI systems, bots, democracy, ethics, and governance. Nevertheless, the sub-themes within these main categories developed as the transcripts were repeatedly reviewed and analysed in greater depth. As a result, the themes was shaped both by the initial insights derived from the literature review, theoretical and legal framework analysis, and by the repeated reading and qualitative analysis of the interview data.

The interviews conducted with the participants were evaluated by dividing them into three subgroups. Subgroup 1 (SG 1) consists of public sector professionals. Subgroup 2 (SG2) includes professionals with experience in NGOs. Subgroup 3 (SG3) comprises those working

most frequently discussed topics by the interviewees. As a result, the themes of democracy, governance and bots are further examined and supported through sub-themes or provided analysis in sub-titles of themes.

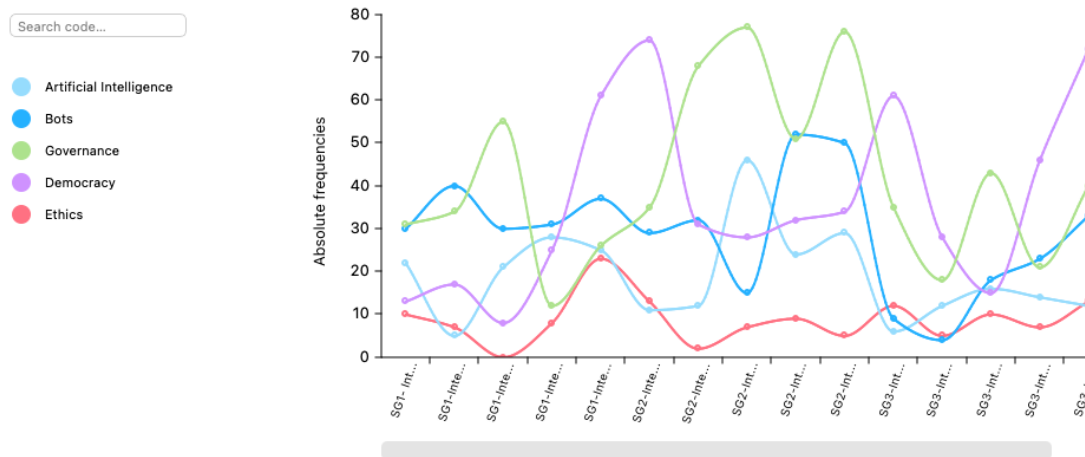


Figure 6. Overview of frequency of main themes referenced by interviewees.

4.6.1. AI Systems

This theme was essential to reflect interviewees' understanding of AI systems. All interviewees were asked how they would define AI. Their responses not only reflected their individual perspectives, but also, reflected their concerns about this technology. Figure 7 and Figure 8 below illustrate the words interviewees used to define AI.

A visual representation, Figure 7, is generated below by Voyant Tools to illustrate the frequency of words used in AI definition by the interviewees. The uploaded text data for this visual piece was not limited to the number of interviewees, namely only 15 definitions were not uploaded. Instead, the responses of interviewees, including the specific phrases and words used by them, were analysed. A According to the corpus, the words used in interviewees' definitions of AI were: tool, making, human, computer, and way.

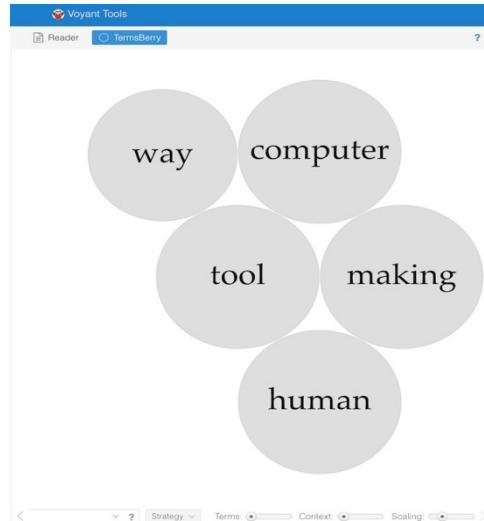


Figure 7. Most frequent words to define AI.

Also, there is another content below that was generated by Voyant Tools (See Figure 8). According to Figure 8 below, the word cloud shows frequently used words to define AI by the interviewees of this research.

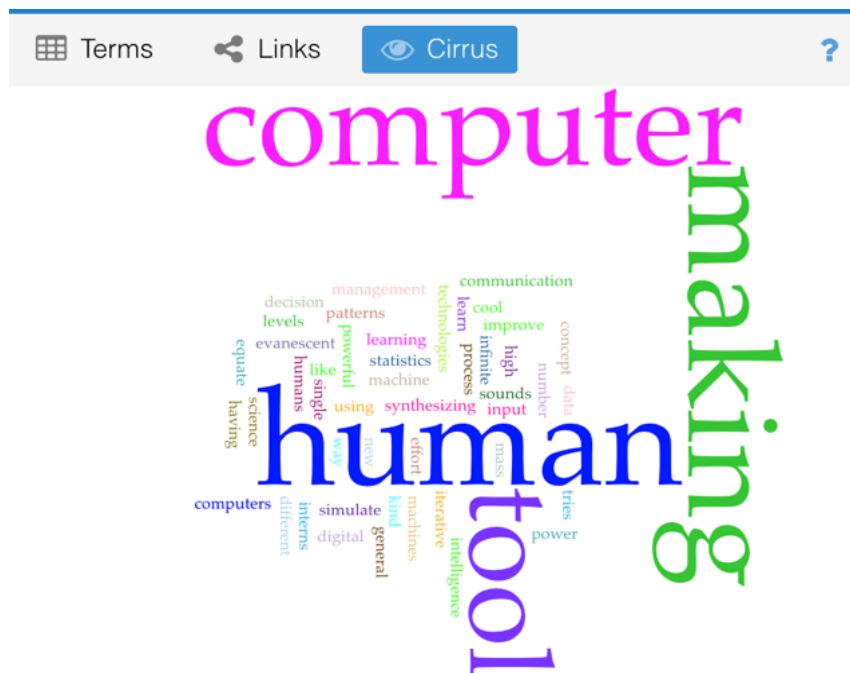


Figure 8. This word cloud reflects the frequently used words.

This visual below, Figure 9, was generated by using Voyant Tools. It presents the co-occurrence of words used by interviewees when they are defining AI. It shows how frequently certain terms, such as tool, human, making, machines and intelligence appeared together. Thus, it highlights conceptual associations made by participants in their descriptions.

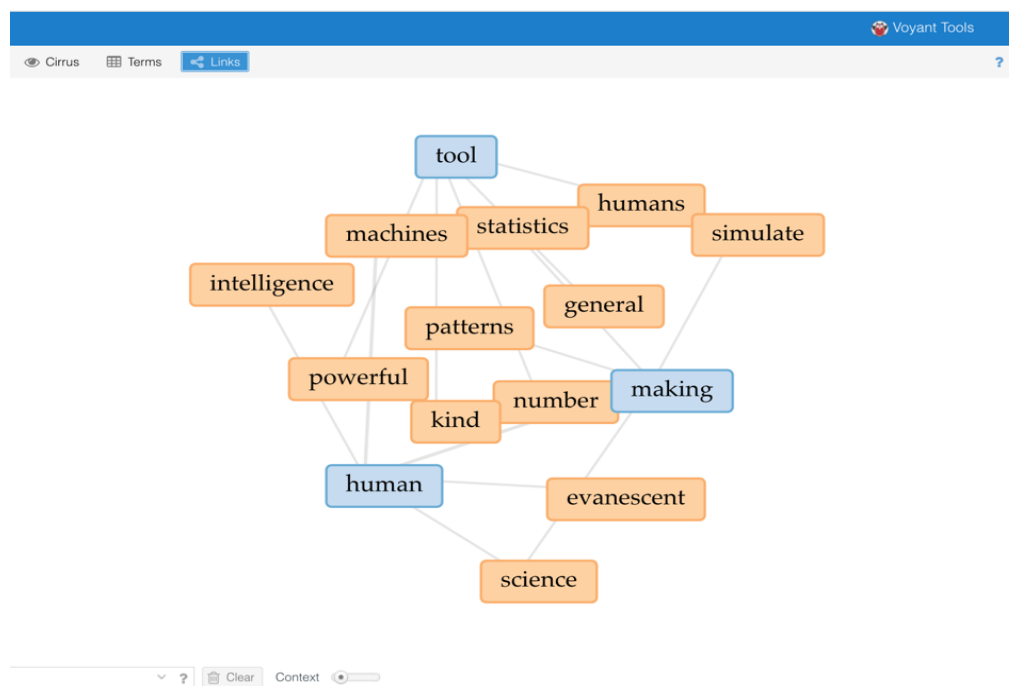


Figure 9. The co-occurrence of words used by interviewees.

Figure 10 presents below anonymised quotations in which interviewees defined AI in their own words and from their perspectives. Based on the responses, AI was commonly defined in the following ways: as a simulation of human intelligence, a statistical process, a form of automation, and as a tool. Additionally, some interviewees described AI as an unclear or ambiguous concept.

Subgroup	Interviewee	AI definition
SG1 (public sector interviews)	Interviewee 1	I would define AI as the science and human effort of making machines and computers simulate human intelligence.
	Interviewee 2	No idea.
	Interviewee 3	Because what AI is very evanescent concept like it doesn't really held by anyone to know what it is. But just the important thing is what it does. Because you can be a lot of techniques. It's not one single thing.
	Interviewee 4	What it is patterns of learning. Okay, so it's a bit decision making approach.
	Interviewee 5	I would define AI as advanced statistics and in general kind of way.
SG2 (NGO interviews)	Interviewee 1	AI is a number of different technologies.
	Interviewee 2	I would define AI as a tool and nothing more.
	Interviewee 3	I don't know.
	Interviewee 4	It's about the mass management of data, okay, on a very high level, the mass management, collation, synthesizing of data using high levels of computer, computer power.
	Interviewee 5	Currently, the way I think of it is like having infinite interns.
SG3 (private sector interviews)	Interviewee 1	I would say an automatically iterative process to improve digital activities, whatever those digital activities might be, whether it's writing or sending ads or that.
	Interviewee 2	A machine which tries to get into communication with humans.
	Interviewee 3	I pretty much equate it with automation. So it's the it's the capacity for a machine to automate a task.
	Interviewee 4	It is a very powerful analytical tool.
	Interviewee 5	AI letter, abbreviation of something that sounds cool, isn't it? Yeah, but I think, yeah. But then from a technical perspective, the new thing is probably the generative AI, where you actually have an algorithm that actually can learn from new input.

Figure 10. Definitions of AI as provided by interviewees.

Accordingly, AI was explained in metaphorical or humorous terms. For instance one participant described it as “*like having infinite interns*” (SG2-Interview 5), while another described it as “*an abbreviation of something that sounds cool*” (SG3-Interview 5). A few

participants also expressed clear uncertainty or discomfort when asked to define AI. They responded with “*No idea.*” (SG1-Interview 2) and “*I don’t know.*” (SG2-Interview 3). These responses seem that even professionals in AI may experience ambiguity in describing what AI actually is.

On the other hand, one of the most frequently used words in interviewees’ description of AI was “tool”. For instance, one interviewee stated, “a tool and nothing more” (SG2-Interview 2), while another described AI as “*a very powerful analytical tool*” (SG3-Interview 4). The first example, in particular, can be noted as a valuable insight because it reflects the approach that intentionally limits the definition of AI to its instrumental function. For this reason, this perspective may be considered instrumentalist. Additionally, there is an aspect that highlights the potential power of AI, particularly in the second quote above.

In contrast, some interviewees pointed to the conceptual vagueness and multiplicity of AI. For example, one participant defined it as “*a very evanescent concept(...) it’s not one single thing*” (SG1-Interview 3), while another described it as “*a number of different technologies*” (SG2-Interview 1). These responses reflect an understanding of AI as context-dependent, fluid, and resistant to fixed categorisation—highlighting the difficulty in pinning it down as a singular, clearly defined entity.

Another perspective reflects a labour-saving approach. Accordingly, a few definitions emphasised AI’s role in repetitive computational functions. For instance: “*I equate it with automation.*” (SG3-Interview 3); and “*An automatically iterative process to improve digital activities.*” (SG3-Interview 1). These participants were interviewees of SG3, the private sector subgroup, and their description may reflect their current professional roles.

Some interviewees focused on AI's computational or statistical capabilities. For instance, “(...)advanced statistics and in general kind of way.” (SG1-Interview 5) and “(...)the mass management, collation, synthesising of data using high levels of computer power.” (SG2-Interview 4). Thus, this framing indicates AI as a tool of efficiency and optimisation. Additionally, the frame reflects its analytical and data-processing power.

Finally, some participants described AI in terms of its capacity to replicate or simulate human cognition. For instance: “(...)the science and human effort of making machines and computers simulate human intelligence.” (SG1 Interview 1); and “A machine which tries to get into communication with humans.” (SG3-Interview 2). These responses reflect a widely-held approach of AI as a form of human-machine mimicry.

Overall, the participants in this study were selected precisely because of their professional engagement with AI-related issues. However, despite their professional backgrounds, participants often focused on different dimensions of AI, including governance, technical development, ethics, democratic risks, or regulatory frameworks. As a result, the interviews revealed limited consensus regarding definitions, terminology, and potential risks associated with AI and political bots.

This finding should not be interpreted as evidence that participants lacked knowledge of AI. Rather, it reflects the rapidly evolving, multidimensional, and highly complex nature of the field itself. AI technologies and their societal implications are developing at a pace that makes it difficult even for professionals to maintain a fully unified understanding.

Accordingly, the absence of consensus among AI professionals constituted an important finding of the research. If even professionally engaged participants diverge significantly in

their understandings of AI-related risks and concepts, this may indicate that such complexities and uncertainties could be even more pronounced for ordinary users and citizens.

Consequently, it appears that reaching a single definition of AI is challenging; the interviews clearly demonstrated this. However, this is not a new finding, as discussions regarding the definition of AI systems are ongoing within the AI Act. There is a tendency among participants to define AI as a “*tool*,” which shows they concretised this concept. This tendency toward concretisation continues in the next section, where their insights are shaped by daily-life practices involving bots.

4.6.2. Bots

In this section, three direct questions were posed to participants regarding bots and political bots. They were asked what they know about bots, how they would think about the use of a bot for political purposes, and what their opinion is on using political bots in elections. In addition to these guiding questions, other reflections shared by participants throughout the interviews were also included, thereby enhancing the analysis of their insights on the theme of bots. The section presents interviewees’ responses and positions the findings in relation to the themes of democracy, ethics and governance, thereby contributing to the evaluations developed later in this chapter.

4.6.2.1. Bot Description

Participants generally provided their responses by drawing on their everyday interactions with bots, and many also referred to their encounters with ChatGPT as a reference point. This, in fact, seems to be a continuation of the tendency to concretise AI-related concepts, as also reflected in the previous section. Also, it becomes apparent that many of their views were

framed within a democratic context. For instance, some referred to bots as tools that can “influence ideas” and “influence public opinion” (SG3-Interview 4, Pos. 174), while others described them as being used “in a non-transparent way that is undemocratic” (SG1-Interview 2, Pos. 30). However, similar to the lack of consensus around the definition of AI, there was no clear agreement on what constitutes a bot and how it functions.

First, bots represent a “slightly outdated concept.” (SG1-Interview 5, Pos. 34). Indeed, the early days of bots, about seven or eight years ago, “chatbots on Facebook or on Messenger as it is now, (...) were like the new thing.” (SG3-Interview 1, Pos. 44-46). It seems the era in which bots operated in a highly coordinated and interconnected manner has largely passed: “My understanding of the part is that the old-school definition of a bot farm dates back to 2016 or 2017, pre-regulation.” (SG1-Interview 5, Pos. 35-39). However, today’s bots represent “a much more complex, multi-organisational approach.” (SG1-Interview 5, Pos. 35-39).

Second, bots are not ‘smart’ in the sense people usually understand intelligence. Instead, they “do things autonomously” and “identify patterns” (SG2 – Interview 1, Pos. 35). One participant complained about bots’ limitations in human conversation, noting that they often try to communicate but failed to truly understand: “this is something I would say who sometimes wants to communicate with me but doesn't understand me.” (SG3 – Interview 2, Pos. 42-43). At this point, the performance of bots was considered largely disappointing. One participant, for instance, commented on GPT-4: “(..)for example, for summarising documents, but so far I have mostly been quite disappointed with the results.” (SG2 – Interview 2, Pos. 33). It appears that even if bots continue to be further developed, they will not reach the kind of genuine intelligence people normally associate with being smart: “I don't think that we will reach anything that is really intelligent in the way that we understand intelligence.” (SG2-Interview 2, Pos. 23).

Even bots are described as *“fake online accounts (...) driven by AI systems or manually by humans that control multiple accounts”* (SG1 – Interview 1, Pos. 15). In some instances, they were even preferred to real humans: *“I’d rather prefer talking to a real person”* (SG3 – Interview 2, Pos. 42-43). They are normally used for practical tasks such as “scheduling appointments, setting reminders, and things.” (SG3 – Interview 3, Pos. 71-75). Namely, the participants preferred *“(..)engaged with bots on a daily basis”* (SG3 – Interview 3, Pos. 71-75), which helped to describe the limits of their knowledge about bots.

Therefore, bots actually make predictions and create the *“impression of doing that very well”* (SG2-Interview 2, Pos. 21). It is even thought that bots have the ability to *“spit out the right sequence of words without any comprehension.”* (SG2-Interview 2, Pos. 23). In addition, interactions with bots can also remain limited due to their repetitive tone and style (SG2 – Interview 4, Pos. 86). As a result, the participants show a tendency to address bots by comparing their abilities to humans in terms of being ‘*smart*’. However, considering the performance of AI-driven bots as merely the result of simple operations producing coincidentally correct outputs would be unfair to the history of bots which is briefly discussed in Chapter 1. But these insights may reflect participants' dissatisfaction with the bots' limitations.

In addition, there is an alternative view suggesting that bots will reach a more advanced level in the near future. The reason lies in the promise of AI to foster more meaningful communication between humans and machines. In these views, AI will enable bots to learn faster and improve their ability to respond to unstructured questions, thereby significantly enhancing their capabilities: *“AI is more a tool for creating meaningful communications between machines and humans. Because AI only helps these bots learn faster and be more flexible in answering unstructured questions.”*(SG3-Interview 2, Pos. 47-49).

Third, the descriptions regarding bots also referred to their use for strategic goals. Accordingly, bots are often used to amplify a message or to support cancel culture tactics. For instance, *“if you want to take somebody down, you just unleash a little bots targeting”* (SG1 – Interview 4, Pos. 31). As highlighted in Chapter 2, bots can make *“a specific message seem as if it is bigger than it actually is, so multiply the effect of this message”* (SG1 – Interview 1, Pos. 15). This very feature explains their widespread and strategic use in political campaign processes within democratic processes. In simple terms, bots are used *“to speed up and improve the process at which we would write a message which has been decided by human beings and approved by human beings.”* (SG3-Interview 1, Pos. 48-51). They might even be used also for *“harass some people that are spreading ideas that are not likeable”* (SG1 – Interview 1, Pos. 15). As a result, bots can be misused in democratic processes or, more generally, for malicious purposes. Through the examples, the participants also assessed the strategic goals that encourage such misuse.

On the other hand, the participants positioned transparency as a response to such strategies. In other words, participants shared descriptions suggesting that promoting more transparent bot interactions could be a way to prevent these strategies. This is explored in detail within the ethics theme. Nevertheless, the use of bots in non-transparent and undemocratic ways was highlighted by participants (SG3 – Interview 5, Pos. 22-23 and SG1 – Interview 2, Pos. 30). This is because bots shape the environment in which ideas are contested and discussed. Indeed, bots were seen as scary tools and this was explained in the context of their mimicking characteristics: *“bots are the real problem, especially if you have a generative AI that can actually mask as being a human a little bit more, then you can really mess with the public space and the legislators in a way that is really scary.”* (SG3 – Interview 5, Pos. 22-23).

These concerns naturally lead to a broader reflection on how bots and new media technologies shape public opinion. By explicitly underlining how new media industries and technologies influence society with the public opinion, participants explained their understanding of bots: *“Bots are basically creating an environment and like visibility of how should I choose my own opinion (...) in the society.”* (SG3-Interview 4, Pos. 174-196). Obviously, this new information ecosystem does not allow for the visibility of plural voices, and the participant complaints about this: *“I just want to see what other things.”* (SG3 – Interview 4, Pos. 174–196).

Finally, in the future, bots are expected to become even more widespread (SG2 – Interview 4, Pos. 67). They are likely to be *“very present and very dangerous for democracy.”* (SG1 – Interview 3, Pos. 37). Furthermore, it appears that *“(..)we're moving towards is just much more interaction with chat bots and AI based chat bots.”* (SG1-Interview 2, Pos. 32). Accordingly, bots have indeed become prevalent, but this expansion has happened somewhat irresponsibly: *“(..) they are now rolled out over society in quite an irresponsible manner because of the limitations that they have.”* (SG2-Interview 2, Pos. 21).

On the other hand, there was a kind of collective response from journalists against the widespread and organised activities of bots: *“all the journalists would share them among themselves, knowing that they are going to get a load of abuse from them essentially in the next day or two.”* (SG1 – Interview 5, Pos. 34). Journalists knew that *“they were all kind of linked.”*(SG1 – Interview 5, Pos. 34). Of course, this collective response was an early measure and limited to smaller circles. Nevertheless, could the prevalence and popularity of bots be somewhat overemphasised? Contrary to common belief, only one participant explained that *“most normal people [are] never exposed to them”* and added that *“those sorts of things people often really overreport”* (SG2 – Interview 5, Pos. 31–32).

Overall, bots were perceived as multi-level and complex tools. Their functional limitations gave the impression that there was a common sense of disappointment among participants regarding the bots. In addition, the participants' descriptions of bots reflected that these limitations were often expressed through comparisons with humans, in which bots were perceived to fail. Participants were also aware that bots are used for strategic goals. These responses reflected an awareness of the broader presence of bots in the public sphere and of their capacity to reshape public opinion. As a response to these strategies, they emphasised transparency. Moreover, one participant shared the example of journalists who had collectively responded to the aggressive strategies of bots, even if manually and within limited circles. This example, in particular, provides valuable insight into collective measures taken against bots in their very early stages.

Subgroup	Bot description
SG1	<i>“sense of a fake online accounts”</i> (Interview 1, Pos. 15)
	<i>“(.)non transparent way that is undemocratic.”</i> (Interview 2, Pos. 30)
	<i>“(...)very present and very dangerous for the monocarcy.”</i> (Interview 3, Pos. 37)
	<i>“to amplify a message. (..) they support a kind of cancel culture that if you want to take somebody down(..).”</i> (Interview 4, Pos. 31)
	<i>“(..)outdated concept(..).”</i> (Interview 5, Pos. 34)
SG2	<i>“(..)do things autonomously and identify those patterns(..).”</i> (Interview 1, Pos. 35)
	<i>“(..)they are not smart in the sense that we understand intelligence.”</i> (Interview 2, Pos. 21)
	<i>“(..)more familiar with than others in online advertising.”</i> (Interview 3, Pos. 27)
	<i>“I know very little about bots.”</i> (Interview 4, Pos. 67)
	<i>“Most normal people never exposed to them(..).”</i> (Interview 5, Pos. 31-32)
SG3	<i>“(..)kind of like a hot and sexy thing. They were like the new thing.”</i> (Interview 1, Pos. 44-46)
	<i>“(..)something (..) wants to communicate with me but doesn't understand me.”</i> (Interview 2, Pos. 42-43)
	<i>“(..)engaged with bots on a daily basis(..)”</i> (Interview 3, Pos. 71-75),
	<i>“(..)creating an environment and like visibility of how should I choose my own opinion (...) in the society.”</i> (Interview 4, Pos. 194).
	<i>“bots are the real problem(..)”</i> (Interview 5, Pos. 22-23).

Figure 11. Descriptions about bots provided by interviewees.

4.6.2.2. Bots in Perspective: Understanding Risks and Responses

This section reflects the perspectives of the interviewees on the risks posed by bots and the potential responses to these risks. It also highlights that participants noted the advantages of bots, yet discussed possible responses to mitigate their negative impacts. Their views are analysed in relation to potential threats, future risks, and capabilities associated with the use of bots in general.

As mentioned in the previous section (5.2.3.1 Bot Description), bots are already highly popular and widespread tools, and they are expected to become even more prevalent in the future. Thus, there is a more complex, multi-layered, and multi-actor landscape, extending well beyond simple single-user, single-account systems to encompass practices such as automation and astroturfing (SG1 – Interview 5, Pos. 35–39). In addition, participants shared some cautious views that focus on the risks and potential misuse of bots’ functions both from a general perspective and in relation to political bots. For instance, a participant remarks “(..)with any technology, there’s always a risk, so it’s how it’s deployed.” (SG1 – Interview 4, Pos. 35). Moreover, this increases the likelihood of bots being used by malicious actors “(..)the problematic uses of that are still going to be affiliated with actors who have bad intentions.” (SG2 – Interview 5, Pos. 35).

From a historical transformation perspective, earlier generations of bots with today’s more advanced technologies highlight that harm persists but in new forms. Accordingly, the main threat lies in the creation of a false reality about how engaged and participatory people appear to be on a certain topic. Several possible threats can be the manipulation of political discourse on specific topics, the use of bot anonymity to disseminate illegal content and the spread of disinformation or hate speech. As the participant explains, “negative consequences and kind of like the risks that emerged with bots in social media is when these bots are used kind of like in a malevolent approach, trying to manipulate the political discourse around the specific topic and trying to kind of like hide behind the anonymity of a bot in order to broadcast illegal content or disinformation or hate speech and kind of like this harmful forms of online expression that are actually more poisoning our democracies than benefiting them.” (SG1 – Interview 1, Pos. 30). Indeed, bots are used to spread misinformation or manipulate public opinion, as Interviewee 4 cautions: “I think it’s where the bots are used to, you know, try to spread misinformation or to damage in a poll, and that’s where we should be concerned.”

(SG1 – Interview 4, Pos. 33). Additionally, bots may adopt biased or discriminatory language over time: “(..)sometimes it goes off and starts to use racist language and so on.” (SG1 – Interview 4, Pos. 35).

However, what enables all this, namely false reality, is the speed and scale of bots. AI significantly accelerates and massively scales up the processes underlying their operation: “*just by virtue of AI, you can push pieces of information through bots out into the scale of millions in a few milliseconds. So I think that’s the computation power that allows for that time.*” (SG2 – Interview 4, Pos. 73–74). Yet, this very speed and scale can also intensify negative consequences, as the participant emphasised: “*AI can exacerbate the negative implications of bots purely by virtue of the scale*” (SG2 – Interview 4, Pos. 76–78).

On the other hand, among the main problems they cause, the participant points first to the way bots “pollute” platforms: “*I think that they pollute Twitter and obviously open up a lot of issues in terms of manipulation.*” (SG2-Interview 1, Pos. 41). This view reflects an expectation of responsibility on the part of the platforms themselves. This “pollution” not only ruins the overall user experience, but also causes the risk that bots make it more difficult to distinguish genuine information from false content: “*(..)they just ruined the user experience and make it very difficult to draw real information.*” (SG2-Interview 1, Pos. 41).

The ability of bots to pollute platforms would also depend on generating a high level of engagement. Therefore, the key indicator of a successful social media strategy is engagement and its continuity: “*So a big part of your successful social media is having lots of engagement.*” (SG3-Interview 1, Pos. 48). Bots, particularly AI-driven bots, serve this purpose by diversifying communication. For instance, bots produce multiple versions of a text message and these outputs can be deployed after human oversight. As the participant explains, this essentially means using bots as a tool to accelerate and refine a message writing process that

remains designed and approved by humans: *“I want to bake the cake myself, but I will use an electric mixer.”* (SG3-Interview 1, Pos. 50).

In addition, the training processes of bots that underpin user experience were also questioned by participants: *“How is it trained? What ethical oversight is there? What risk assessments are done?”* (SG1 – Interview 2, Pos. 32). Indeed, people are likely to interact more frequently with chatbots and AI-driven bots in the future. However, there will remain two reasons for the advancement of bot-based technologies: reliance on LLMs and the data quality. Above all, the future of bots depends less on AI as a program or system and more on the quality of data and data annotation: *“AI absolutely can have a huge impact, but I would say specifically that the data contained within the AI is the key.”* (SG3-Interview 3, Pos. 81). On the other hand, the importance of ethical oversight, transparency in training processes of bots and AI systems, and risk assessment will remain as concerns that typically arise whenever new technologies are introduced. As a result, such concerns can be addressed through careful planning, ethical principles and a structured approach.

In another respect, the interviews reflected profiling and customised advertising as future risks resulting from advanced AI-driven systems. For instance, Interviewee 3 noted *“(.)you don't need AI to make both fraud work, but AI will trigger in the ad market a whole lot of stuff about them customizing the ads.”* (SG2-Interview 3, Pos. 27). In addition, a more significant future risk is the potential misuse of customised advertising through profiling. One participant highlighted this risk, noting that *“(.)that's a very niche example of a bot, but you can see how a system that can quickly recognise traits in a person and then quickly come up with a visual to suit. That person could be exploited for that system.”* (SG2-Interview 3, Pos. 27).

Finally, threats and risks to democracy arise when bots are used in political campaigns. Although these risks and their detailed analysis are discussed in the next section, the interviews

already highlighted significant concerns regarding political communication. The generative AI make political bots appear human-like and thus highly manipulative. Thus, bots could distort public spheres and legislative processes in significant ways (SG3-Interview 5, Pos. 22-23). For instance, by infiltrating open-access panels for market research or political polling, bots could artificially promote a party and create a false narrative of support : *"(..)you have a lot of influence from bots there as well. If you hijack that, you could boost the party and create a false narrative about a winner party which is not, and once again use the traditional media to create this false public opinion or drive for legislation for an issue that is not there, and that is quite an effective thing."* (SG3-Interview 5, Pos. 22-23).

On the other hand, even a momentary failure of human oversight regarding bots could generate major risks, potentially finishing a political campaign: *"If you get perceived that all of your social media engagement is by a (..) bot, like that's it, you will never, you will never win a seat again."* (SG3-Interview 1, Pos. 51). However, as mentioned by one participant, *"(..)every country has their own interests, and after all these globalisation processes."* (SG3-Interview 4, Pos. 220). There is a limitation, such as certain opinions can be influenced, but others remain the same because of the rational choices, party identity, or ideology (SG3-Interview 4, Pos. 220). As a result, the influence of bots in political communication carries a significant risk for electoral results.

Participants suggested bot detection systems as a response to these current and future risks. This is because bots can rapidly become more sophisticated and increasingly difficult to detect: *"there is a level of sophistication that I can give to bots in a way that they become really hard to detect as bots and also the rules that they operate on can become more and more complex."* (SG1 – Interview 3, Pos. 51–53). However, the platforms may become more successful in identifying and excluding bots: *"(..)their effectiveness is extremely limited now because of how*

high, quick and easy the mainstream platforms are.(..) and identifying them and knocking them out.” (SG1 – Interview 5, Pos. 35–39). Thus, AI could also be deployed to improve detection: *“for online platforms it could become easier with the AI to detect them so.”* (SG1 – Interview 3, Pos. 57). As a result, while detecting bots can be very challenging due to their sophisticated characteristics, the use of AI could also make detection easier in the future.

Overall, across the three participant groups, SG1, SG2, and SG3, the general tendency was to approach bots with caution. Participants identified current risks associated with bots, particularly the spread of disinformation, misinformation, and hate speech, which together contribute to the concept of a false reality. In addition, they shared insights regarding future risks, such as those related to personalised advertising and profiling. Bot detection systems were positioned as a response to these risks. However, as bots continue to advance, these systems appear increasingly ineffective. Some participants, nonetheless, suggested that detection could become significantly more effective once integrated with AI models, though there was no clear consensus on this point.

Taken together, the analysis suggests that the capabilities and limitations of bots ultimately reflects a broader tension between two competing narratives: one portraying AI as an inflated bubble rather than a revolutionary force, and the other viewing it as an irreversible breakthrough, *“the genie out of the bottle.”* (SG3-Interview 3, Pos. 127). As a result, this analysis of bots effectively outlines the broader framework of the ongoing debate on whether AI represents a truly revolutionary force or not.

4.6.2.3. Bots in the Political Sphere

Participants were asked about their views on the use of bots for political purposes during democratic processes. Overall, two-thirds of participants, 6 out of 15 participants, expressed supportive perspectives regarding the use of political bots in democratic processes. Three out of five participants in SG1 expressed their supportive perspective regarding the use of political bots in elections, however, there was no consensus among interviewees in SG2. While three interviewees express negative views, two others present with different reasons for considering the use of political bots in elections as not necessarily a bad thing. In SG3, only one participant expressed a positive view regarding the use of political bots. Thus, the majority of participants across the three sub-groups did not reflect positive views regarding the use of political bots in democratic processes.

The one-third of the participants stated that political bots' capabilities are limited in electoral processes. Similarly, three out of five participants in SG1 agreed that the capabilities of political bots remain limited for electoral purposes. This emphasis on limited capabilities was also echoed by Interviewee 1 and Interviewee 2 in SG2, but found no support within SG3.

From a broader perspective, participants share their views on whether political bots can influence electoral processes. Even this is a question as *“an empirical question that can be answered statistically”* (SG2-Interview 1, Pos. 53), it is found as *“incredibly interesting and complex”* (SG1- Interview 1, Pos. 36). As a result, participants' responses extend to considerations of democracy, ethics, media, and digital platforms. However, these reflections are analysed under separate themes in later sections.

4.6.2.3.1. Supportive Perspectives on the Use of Bots in the Public Sphere

Accordingly, participants were supportive because they think that political bots can be effective in democratic processes (SG1-Interview 3, Pos. 77) There is no reason to avoid using them in elections (SG1-Interview 2, Pos. 34), in contrast, using political bots in campaigns could be reasonable (SG1-Interview 4, Pos. 45). For instance, “*(...), but if this tool [bots] is operated by a good person and genuine person, then it can give a lot of benefits for a democratic process.*” (SG3-Interview 4, Pos. 260). Moreover, bot practices and automating the dissemination of information through bots could be beneficial (SG1-Interview 2, Pos. 43). Indeed, political bots can serve as useful tools for elections and political parties as long as users are aware that they are interacting with a bot (SG1- Interviewee 1).

As for the influence of political bots on electoral processes, participants believe that such bots have no direct influence on election results or this is “*the great unknown right now*” (SG3-Interview 1, Pos. 59). In particular, they described these technologies as “very disruptive,” but argues that there is no evidence that bots have *swayed* elections (SG1- Interview 1, Pos. 37). Even if political bots could have an influence on elections, their impact is often overstated: “*The flip side of that is I think some of the research (...) really overplays the impact of bots.*” (SG2-Interview 5, Pos. 50). Namely, reliance on bots is not feasible, yet this does not lead them to categorise accepting political bots as “bad” (SG2-Interview 3, Pos. 29). The reasons provided include the low quality of bots—even when AI-driven—and the fact that it is usually easy to understand when one is interacting with a bot (SG1- Interview 1, Pos. 37). It is even possible to assume that people are “*quite aware*” of *such* bots and therefore tend to dismiss them and refrain from engaging with them (SG1-Interview 5, Pos. 54).

As a result, political bots are considered to have very limited impact on electoral campaigns, with no evidence of influencing outcomes (SG1- Interview 1, Pos. 39). Even the interaction of

bots could be limited for participants (SG2-Interview 4, Pos. 86), their role is found as meaningful in providing a “*plurality of voices up to the consumer to evaluate and have more informed choices*” (SG2-Interview 4, Pos. 104–105). In particular, this is “*much better than having one voice being thrown out by centralized governments*” (SG2-Interview 4, Pos. 104–105). Thus, this approach appears to run parallel with Habermas’s view, in Chapter 3, that the political public sphere can only be established through well-informed individuals.

A participant, Interviewee 2 supports this perspective, highlighting that the more interesting issue lies in the perception of bots: “*the perception of bots has more of an effect than bots themselves.*” (SG1-Interview 2, Pos. 49). Indeed, this perception of bots persists like a ghost wandering across platforms, even when they do not actually exist. The reality is not immediately apparent, as it is often unclear whether there are real individuals behind these accounts. It seems the real challenge is the confusion between bots and human users. As an example, this participant refers to Sinn Féin bots, which have few followers and no profile pictures, but nevertheless mimic pro-Sinn Féin during certain events (SG1-Interview 2, Pos. 47). However, this illustrates that political bots are relatively easy to detect because of (1) their obvious features, (2) their poor convincing capacity, and (3) their language use—often adopting an American style of communication (SG1-Interview 2, Pos. 47).⁶⁵⁹ As a result, bots are frequently “imported”, and may not align with the cultural and linguistic contexts of every country.

⁶⁵⁹ To see more on how internet interaction in Ireland has often followed American patterns, see Gallagher (n 62).

4.6.2.3.2. Critical Perspectives on the Use of Bots in the Public Sphere

On the other hand, political bots are perceived to pose a threat to democracy (SG2-Interview 5, Pos. 61). To put it simply, the use of political bots is “*not a good idea*” (SG3-Interview 2, Pos. 62); it is “*risky*” (SG3-Interview 3, Pos. 106) and represents a “*real danger*,” particularly when combined with generative AI (SG3-Interview 5, Pos. 27). Therefore, participants struggled to show a positive example of bots being used for political campaigns, adding that there is no “*upside for society*.” (SG2-Interview 1, Pos. 42 and Pos. 44). A participant finds the matter “*very worrisome*” (SG2-Interview 2, Pos. 56). Because there is a concern about if ‘*political bots make mistake*’ even they are used in a ‘*well-designed*’ web page (SG2-Interview 2, Pos. 39).

Thus, the central concern remains as the use of personal data (SG1-Interview 5, Pos. 52), and it is required a balance with the bot use and protection of privacy rights (SG1-Interview 4, Pos. 39). The clearest illustration of the potential impact of political bots can come through the example of Cambridge Analytica, which a participant described as “*very damaging to democracy and to electoral processes*” (SG2-Interview 2, Pos. 58 and Pos. 62). Therefore, it is necessary to ensure that bots are not employed “*for the purposes of undermining the electoral process or for misinformation or disinformation*.” (SG1-Interview 4, Pos. 45). Because their activities are regarded as deceptive (SG1-Interview 3, Pos. 76).⁶⁶⁰ Indeed, a participant draws attention on this: “*As AI gets better and the LLMs are getting smarter and the risk of deception gets higher*” (SG3-Interview 1, Pos. 58). In the same way, participants acknowledge bots'

⁶⁶⁰ Despite providing an oversight-focused definition, the Code of Practice for GPAI defines deception as “model behaviours that systematically produce false beliefs in others.” See details ‘Code of Practice for General-Purpose AI Models’ (n 475) 29.

cleverness, for instance, noting how they avoid political websites and instead intervene in “*indirect political discussions.*” (SG3-Interview 2, Pos. 69).

In addition, bots can “hone” the messages, including false messages, being circulated, thereby increasing their influence in elections (SG1-Interview 4, Pos. 41). Even with limited use, however, political bots could increase “*the volume on the load and the frequency of political campaigning.*” (SG1-Interview 5, Pos. 43).

Political bots create false virality (SG1-Interview 5, Pos. 78). Moreover, the overwhelming amount of informational noise in the political communication environment diminishes the efficiency of any such technologies (SG3-Interview 4, Pos. 235–238). This suggests that the perceived impact of political bots is limited not only by their own capabilities but also by the wider, often unhealthy, information environment in which they function. For instance, their effects are more evident in referenda rather than in elections, particularly in controversial referenda such as Brexit (SG1-Interview 4, Pos. 43).⁶⁶¹ Because political bots are capable of changing “*a bit the sentiment over a certain political personality or a certain political party.*” (SG1-Interview 3, Pos. 77). Yet, even more important is the scale of use: the extent to which bots are deployed is key to determining their impact on public perception: “*the scale is key to change sentiment.*” (SG1-Interview 3, Pos. 77).

There is also another possibility regarding the influence of political bots. Recommender systems could contribute to political polarisation: “*Recommender systems have helped to polarize the voter, so there is fewer swing voters in the middle. People are moving to the*

⁶⁶¹ The interview questions did not focus on the Brexit, the 2016 US elections, or specific referendums in which political bots were employed. The study clearly defined its jurisdiction as the European Union and the case law of the CJEU. Nevertheless, interviewees occasionally referred to the Brexit referendum in their examples. The interview questions were designed as open-ended to avoid directing such references. Also, the interview questions are provided in the Appendix.

extremes.” (SG2-Interview 3, Pos. 61) This very insight, in fact, underscores how electoral strategies are increasingly built upon delicate calculations centred on polarisation.

From a similar perspective, another participant also highlights the potential impact of political bots on public opinion, from a perspective parallel to Habermas’s emphasis on a well-informed public sphere (See more in Chapter 3). The participant, Interviewee 4 explains: *“If you have a huge number of advertisements on a certain candidate reaching many people, and those messages are designed to attract certain types of people, it can have a big influence. (...) I think it is up to the population then to be able to distinguish what’s about, what’s not about. And that’s an education aspect”* (SG2-Interview 4, Pos. 113). In this sense, bots may accelerate the tempo of campaigns and contribute to shaping momentum. (SG3-Interview 4, Pos. 235–238). These insights clearly highlight the importance of AI literacy. At the same time, it shows the difficulty of measurement, as previously reflects above in relation to the concept of scale. the question raised regarding the influence of political bots is: *“How can we measure it?”* (SG2-Interview 4, Pos. 151–152).

Indeed, there is a challenge of quantifying such influence, and a participant points out that a parliamentary constituency has about 65,000 voters, only some of whom are active on platforms such as Twitter (SG2-Interview 5, Pos. 52). As a result, the views of Interviewees 4 and 5 make it evident that measuring the influence of political bots is, in itself, a major challenge.

At the same time, there are reputational risks for political parties that rely on bots in elections, emphasising that such use will inevitably “have a cost” (SG2-Interview 5, Pos. 47 and 61). Parties with a genuine chance of success in elections are unlikely to hire bot networks; rather, the hiring of political bots is more likely to occur in “like authoritarian or semi-authoritarian countries.” (SG2-Interview 5, Pos. 47).

4.6.2.3.3. Practical Pathways for Bot Governance

Both positive and negative insights indicate that political bots, regardless of their use in elections, will always require human oversight: “(..)it is going to have to be a person at PR, person, party political, a marketing person, somebody in a particular role that is going to have to tell the language learning model, what to produce, tell the AI what to produce and tell it how to campaign.” (SG1-Interview 5, Pos. 43). Another point relates to methods of political communication. Honesty and integrity were emphasised as the most effective ways to engage with voters: “I really believe that the best way to sell a candidate is to make people understand that your best weapon is being honest, to keep your integrity in place. Talk about things that you really believe in and voters can feel it.” (SG3-Interview 4, Pos. 252–253).

Thus, the participants, especially the majority in SG3, highlighted that face-to-face communication remains essential for winning elections. As one participant put it: “For winning, you need to motivate and touch people with their emotion. And this you can do face to face. I mean it’s very difficult doing it in a different way” (SG3-Interview 2, Pos. 131). Another highlights that what truly wins elections is the “*feeling of normalisation of discourse and conversation*” within personal networks (SG3-Interview 1, Pos. 59). Indeed, the negative influences of political bots discussed above derive from a real concern about whether “*an LLM bot [can] be used to sort of plant language and to create a sense of normalising rhetoric,*” and “*[it] is a fear.*” (SG3-Interview 1, Pos. 59). At this point, this concern becomes real, as it is argued that when combined with generative AI, “*[political bots] could start shifting public opinion because politics is going so fast now, because that is not value-driven, it is more populist driven*” (SG3-Interview 5, Pos. 27).

As a result, “*We are heading into times where people will value face-to-face communication more again*” (SG3-Interview 2, Pos. 119). Indeed, the analysis of whether political bots

influence elections and how their use is perceived within democratic processes cannot be separated from broader dynamics of political communication, political campaigns, media influence and media environment. In conclusion, elections are not won merely through the presence of political bots. Traditional practices remain influential, such as the continued importance of traditional media and face-to-face engagement with voters. This insight ultimately highlights that where the human factor is central, technological automation alone does not determine electoral results.

4.6.2.4. Effectiveness of Existing Legal Frameworks in Governing Political Bot Usage

In this section, participants address the effectiveness of the legal framework. They highlight its inadequacy in addressing political bots, and often link these limitations to concerns about freedom of expression. Another concern is the legal uncertainty surrounding “bot speech” and how it should be regulated. Thus, the overarching question that has been how bot speech could be regulated. Participants also draw attention to the interconnected challenges of power asymmetries, lack of expertise in public authorities. Together, these difficulties cause a complex structure that undermines regulatory effectiveness.

For SG1, the very lack of consensus here may be itself a finding. The participants in SG1 are public sector employees, including academics in the universities in EU, rapporteurs in European Commission, and politicians. They could be expected to have more detailed knowledge of the legal framework than participants from other groups. This is because some participants in SG1 were directly involved in the development of the AI Act as rapporteurs. Also another participant in SG1 was politician at the national level (in Ireland), so the participant were already working on compliance and implementation issues related to the AI Act. In addition, participants from academia were actively researching these topics and, in

some cases, contributing public feedback during consultation and Commission-related processes. Therefore, their detailed knowledge was considered capable of providing particularly valuable insights for the research.

The only major tendency across their views is the recognition that, while there are already many tools within the current legal framework, further regulations are still required. This also suggests that the frequent criticisms directed at the EU for over-regulation may not be entirely unfounded. In SG2, participants' reflections are shaped primarily by concerns about freedom of expression, and their knowledge of the legal framework appears to be more general compared to SG1. So, the insights gathered on the effective legal framework for political bots seem deeply interlinked with the other themes of this chapter, such as governance, media, and democracy. In SG3, all participants agree on the necessity of regulating political bots. However, four out of five participants immediately add a caveat: they are uncertain about how such regulation could be implemented, either because controlling bots is perceived as highly difficult or because of the potential contradiction with freedom of expression.

Accordingly, there are already "*a lot of tools*" available within the current legal framework (SG1-Interview 3, Pos. 77). However, political bots should be regulated '*towards political parties*' (SG2-Interview 2, Pos. 70). Because the AI Act still has some '*loopholes*' (SG2-Interview 2, Pos. 95). Accordingly, due to the absence of specific legal provisions on bots (SG2–Interview 4, Pos. 108), regulatory constraints are considered necessary (SG1–Interview 1, Pos. 46). It seems this is a '*result of negotiations*', and that *always happens in regulatory processes: 'loopholes'* (SG2-Interview 2, Pos. 95). This might also be a result of power asymmetry and could be related to the ineffectiveness of the AI Act for political bots, as it is considered "*a very complex law*" (SG2-Interview 2, Pos. 95). Nevertheless, when there is

enough willingness, funding, and creativity, actors can always find ways to bypass restrictions. (SG3–Interview 4, Pos. 232).

Another problem might be that *‘many supervisors are under-resourced’* (SG2-Interview 2, Pos. 95). Furthermore, politicians are not necessarily *‘experts in the technology and in the social implications’* (SG2-Interview 2, Pos. 95). This insight directly linked the legal debate to broader themes of governance, power asymmetry, ethics and implementation difficulties.

On the other hand, the idea that the AI Act intervenes on political bots to a certain extent finds support among the participants (SG1-Interview 3, Pos. 77). However, a further concern about the potential effectiveness of the legal framework for political bots under the AI Act derives from the lack of substantive enforcement of the GDPR and the description of this regulation as a *“crisis.”* (SG2-Interview 3, Pos. 71).

Nevertheless, there is acknowledgement that the rapid development of AI, especially general-purpose models, had not been fully anticipated in earlier regulatory proposals (SG1–Interview 3, Pos. 61). In line with the analysis presented in Chapter 3, a participant (SG1-Interviewee 3) adds that when the European Commission published the proposal, there was nothing on general purpose AI in general (SG1-Interview 3, Pos. 61). What is particularly interesting is the lack of awareness regarding how powerful models could be, not just in terms of bots specifically, but in terms of AI capabilities overall (SG1-Interview 3, Pos. 61). Therefore, concerns are also raised about whether legal frameworks can ever keep pace with current technologies or future technologies, with one participant noting that *‘government will always be on the back foot’* (SG3–Interview 1, Pos. 63). As a result, uncertainty and lack of confidence remain regarding the effectiveness of the current legal framework.

However, transparency rules, “*which are kind of the essence of what some of the regulations around elections [are]*” (SG1-Interview 2, Pos. 51), are seen as a potential solution to this uncertainty. Thus, regulation in political campaigns should focus on transparency rather than content (SG2-Interview 5, Pos. 58). Indeed, political parties must ensure transparency when using AI bots (SG1-Interview 1, Pos. 48). In particular, transparency requirements on advertising are viewed as a useful model: “*So with advertising, there are transparency requirements. I think the same thing should exist for bots, just be sure transparent about how are you using them, in what context to at what scale.*” (SG1-Interview 2, Pos. 51).

In addition, bot speech remains within a grey zone, as discussed in detail in Chapter 3. Concerns about freedom of expression also reappear in the political bots context (SG3-Interview 2, Pos. 73–75). Accordingly, it might be possible to equate bot speech with *indirect* human speech, raising doubts about the AI Act’s ability to adequately address political bots (SG2-Interview 1, Pos. 45 and Pos. 66). These concerns are accompanied by reflections on competing regulatory approaches between strict privacy protection and strict control, neither of which provides a clear solution (SG3-Interview 2, Pos. 80–81). Thus, an effective regulation would depend on cooperation across platforms, electoral commissions, political parties, and the public. (SG1-Interview 4, Pos. 58)

4.6.3. Democracy

4.6.3.1. Democracy: An Overview

Participants are aware that democracy is under threat from new technologies. They also recognise that democracy is vulnerable to manipulation through political bots and AI technologies in democratic processes, and they express concerns about this. However, there is no consensus on the exact nature of these threats or on potential solutions. Even though

participants come from different sectors, they do not put forward a common remedy or a clear root cause.

For instance, SG1 participants were contributing rulemaking process at national and international level regarding AI systems. They actively involved in legislative and regulatory processes. However, the participants in SG1 did not converge around a common understanding of democratic threats arising from the regulation of AI systems. The approaches of SG2 participants to interview questions primarily from a rights-based perspective. However, it did not overlap with the views of SG1. The same applied to SG3 participants, who were either directly involved in or closely observing the practical use of AI systems in democratic processes. Accordingly, the absence of a common remedy or a single root cause itself emerged as a significant finding.

Accordingly, the lack of consensus itself constituted an important finding. The participants were highly educated, and all had at least university-level education. They also had professional engagement (at least) with AI. Nevertheless, they did not converge on a common understanding of threats to democratic processes or on possible solutions to those threats.

What is particularly interesting is that SG3, the private sector, does not share the belief that technology alone poses a threat to democracy. Instead, they emphasise that elections are not won by political bots on their own, but face-to-face communication remains at the heart of political communication as discussed in Section 5.2.3.3, Bots in the Political Sphere section.

Participants stated that democracy has been influenced by a '*technological storm*', where citizens are required to cast their votes in an environment of '*unchecked technology*'. (SG2-Interview 2, Pos. 91). The effects of these technologies are described as '*overall negative*' (SG2-Interview 1, Pos. 46). This is because political bots and the driving technologies behind

them as clearly *harmful* for democracies (SG1–Interview 1, Pos. 30), *undemocratic* due to their lack of transparency (SG1–Interview 2, Pos. 30), *dangerous* (SG1–Interview 3, Pos. 78–80), *undermining the democratic process* (SG1–Interview 4, Pos. 54), and as technologies that have *utterly transformed democracy* (SG1–Interview 5, Pos. 52).

Indeed, as AI systems become increasingly powerful, the potential for manipulation through bots and large-scale AI-driven political campaigning has become a very real concern (SG2–Interview 1, Pos. 78, Pos. 70, Pos. 46, and Pos. 69). For instance, if the bot is spreading malicious information, then it should be removed from the platform, even at the expense of freedom of expression (SG2–Interview 4, Pos. 215). However, an important distinction is made here: society does not mean platforms (SG3–Interview 1, Pos. 59). The quality control in information should meet the highest standards for the society; but, it appears that technology companies are failing to take this issue seriously. One participant found this attitude of the platforms offensive, describing the current environment as living in “a kind of wild west” (SG3–Interview 3, Pos. 138).

Concerns about democracy also intersect with the role of political party funding (SG2–Interview 4, Pos. 213–215). Financial limits on funding political parties are necessary to protect democracy (SG2–Interview 4, Pos. 213–215). However, political campaigning, as a well-organised industry, has shifted as it is increasingly driven and enhanced by social media and digital technologies. For instance, face-to-face interviewing still matters, even if it has become increasingly expensive (SG3–Interview 2, Pos. 119). Thus, political parties may rely on “*armies and bot armies*,” surveys conducted face to face with real people are still crucial because only a representative sample drawn from actual respondents can provide “*representative public opinion*.” (SG3–Interview 2, Pos. 119). As a result, public opinion remains the foundation of democracy, and everything else is built upon it.

On the other hand, a direct correlation can also be seen between public opinion and trust.⁶⁶² Accordingly, democracy, elections, and campaigns are processes built on trust. Instead of building public trust, political campaigns often prioritise undermining the opponent's credibility: *"it is easier to demobilize your enemy's voter base than to build trust. Destroying trust is so much faster. So, negative campaigning is what works in the end because you don't have that much time—building trust takes so much time"* (SG3–Interview 5, Pos. 53). Consequently, this strategy is likely to shape and polarise public opinion.

As a result, a *technological storm* is transforming democracy, political parties, and campaigning alike. Bots are particularly trained for the relationship between public opinion and public trust and they identify this relation. This is why political bots are often employed to manipulate democratic processes. Another key finding from the interviews is that, even where freedom of expression clashes with the protection of democracy, consider that the greater goal is to protect democracy, even if might require suppressing the "voice" of political bots.

4.6.3.2. The Media Environment in the Age of Political Bots

As noted in Chapter 2, this theme, democracy, also seeks to analyse the role of the media, which is traditionally seen as a watchdog of democracy. This role of media within the transformed and multi-actor environment has been shaped by political bots and emerging technologies by drawing on participants' insights. In the context of democracy, this theme also connects with other sub-themes such as media, media blackout, and media influence.

Media blackout refers to a short period during democratic processes in which media coverage related to the election, candidates, and campaign activities is paused to allow voters to reflect and make decisions in a well-informed and unbiased manner. The critical period lies in the 24

⁶⁶² Reisach (n 359) 907 and 908.

hours before the election, because “(...)lots of claims [are] getting pushed out, often lots of *disinformation*.” (SG1-Interview 2, Pos. 80-81). The primary aim of this period is to prevent individuals’ pre-election decisions from being manipulated, and to enable citizens independent choices. This concept supports the idea of a broader role assigned to media as one of the pillars of democracy.

One of the most important findings of this research is that some participants had never even considered the possibility that social media, as a form of media, should also be included in the scope of media blackout before elections. In SG1, most participants, 4 out of 5, believe that a media blackout would not be feasible to implement in online environments. SG2 participants provided limited input on this issue, while SG3 offered valuable reflections on the current media environment, even without directly addressing media blackout.

Indeed, some participants never considered the possibility of a media blackout in new media (SG1- Interview 1, Pos. 80, SG1-Interview 2, Pos. 80-81, SG2–Interview 4, Pos. 184–185). However, they also supported that a media blackout should also apply to social media (SG2–Interview 4, Pos. 168). Because the platforms are also media, the current situation is inconsistent (SG2–Interview 4, Pos. 168). On the other hand, a blackout in this media environment could present a significant opportunity for political bots to fill the gap (SG1-Interview 1, Pos. 86-87). Thus, if platforms count as new media, then they should be fully adapted into the broader media category, just like television (SG2–Interview 4, Pos. 168).

Also, there are some variations in how participants conceptualised the idea of a media blackout. For instance, some find the term media blackout to be “*scary*,” instead preferring the phrase “election silence.” (SG1-Interview 3, Pos. 100). Some suggest that “*media sensitivity*” is a more appropriate term (SG1-Interview 5, Pos. 123). Drawing on this concept, it argues that any attempt to apply blackout measures across all platforms and electoral regions may face

jurisdictional ambiguity (SG1-Interview 5, Pos. 123). Moreover, the implementation of this concept may likely vary from one platform to another, such as Facebook and TikTok (SG1-Interview 5, Pos. 119-120). Even if a platform removes certain content, a few users may still view it before the removal is enforced (SG1-Interview 5, Pos.120). Nonetheless, *“this kind of question of media sensitivity is really important on mainstream platforms, public facing platforms.”* (SG1-Interview 5, Pos. 123).

On the other hand, the media landscape has changed over the past two decades (SG3–Interview 3, Pos. 130–131). Accordingly, the key finding is that the power of traditional media has been eroded. This is because traditional media, by its own hand, gave credibility to distorted or manipulated content from new media. For instance, a participant shares a critique of traditional media, *“the newsrooms are very focused on looking at the feeds in social media. (..) which means that you can address the people more by the algorithms fooling traditional news media could then feed stuff to out to the general public.”* (SG3-Interview 5, Pos. 22-23). And yet, elections cannot be won without traditional media, and this stands out as a crucial insight of the study. Media continues to be a decisive factor in winning elections (SG3–Interview 5, Pos. 38), and without traditional media outlets, and especially television, electoral success seems impossible (SG3–Interview 5, Pos. 37).

Namely, these insights lead to an important finding: minor parties may use bots to reach more people, but they cannot win elections this way. At best, they can secure visibility within the democratic processes. Similarly, while influencers may be used for manipulation, their impact on election results remains limited (SG3–Interview 5, Pos. 38). In fact, this also provides a partial answer to the question raised in Chapter 2 about whether influencers could meaningfully affect election results.

By contrast, the current position of journalism appears far less clear. While some still expresses belief in the importance of *independent and verified journalism* (SG2–Interview 2, Pos. 87), others emphasise the *collapse of journalism* in the new media environment (SG2–Interview 3, Pos. 75). Traditional media depends on its audience for survival, yet “*audience leakage [which] is a cancer at the heart of journalism*”, and ultimately results in “*a collapse of information in democracy*” (SG2–Interview 3, Pos. 75). However, a democratic media environment could still be possible if transparency is encouraged (SG2–Interview 5, Pos. 58). Otherwise, the risk remains of a system where every voter can be profiled and elections can be manipulated (SG2–Interview 5, Pos. 58).

Thus, it seems people will continue to rely on broader signals of trust and maintain confidence in traditional media: “*people still largely continue to lean on bigger signals of trust... they still use the media... people actually trust the media a little bit more than is thought and are not going to believe the first thing they see on the internet.*” (SG2 – Interview 5, Pos. 36). Yet, as one participant put it, “the genie is already out of the bottle” (SG3–Interview 3, Pos. 132–135). What can be put back into the bottle is very limited, and solid quality control mechanism over information no longer exists (SG3–Interview 3, Pos. 132–135). Namely, one can interact with bots as a citizen, researcher and as someone who wishes to get informed ‘*just like about all things current affairs.*’ (SG1–Interview 1, Pos. 21) However, potential risks to the quality of the information are linked to the AI literacy as well.

At the same time, the question of what function new media now performs in place of traditional media arises. New media “*creates a business model for the worst material.*” (SG2–Interview 3, Pos. 75). Namely, the worst material is any content. Yet this model remains closely linked to the freedom of speech (SG3–Interview 5, Pos. 72). This is because new media acted as an intermediary and functioned as a kind of auditing of power on behalf of the people at the

beginning of the internet. But these new media outlets now increasingly ignore this responsibility (SG3–Interview 5, Pos. 72). Nevertheless, due to the implementation of intermediary policies, the presence and impact of bots have become constrained. For instance, “(..) *five years ago you would have seen an awful lot more BotNets as a media monitor. (...) that type of bot is limited and has limited impact.*” (SG1 – Interview 5, Pos. 35–39). As a result, platforms took advantage of the unstructured space offered by the complex business model they introduced as new media during the early stages of the internet. Today, they are attempting to reshape the responsibilities arising from that same model to fit their own interests.

4.6.3.3. Platform Responsibility in Relation to the Functions of Political Bots

Platforms are expected to comply with ethical principles, criteria and standards (SG2–Interview 4, Pos. 196). While no participant explicitly argued that platforms should bear direct responsibility because of algorithmic speech, they all acknowledged the ambiguity of responsibility and highlighted the need for clarity (SG3–Interview 3, Pos. 127). In addition, Beyond their colonial position in dominating competition in the market, the interviews reveal widespread concern that platforms leverage their asymmetric power to gain advantages globally, particularly in relation to countries outside Europe, such as China (SG2–Interview 3, Pos. 76–78). Across all sectors, participants underline the need to defend or at least remind dominant actors of ethics, responsibility, and the law, even in the face of colonial positions and power imbalances.

The primary aim of platforms is to capture attention. Because they already depend on user interaction, yet bots actually reduce engagement; with Facebook cited as a notable example (SG3–Interview 1, Pos. 58). Thus, platforms now “*need to be extremely careful about what [they] allow and what [they] don’t allow*” because of the intensity of bots and their interactions

(SG3–Interview 1, Pos. 58). Due to the bot pollution on platforms, people are driven to “authentic communication” (SG3–Interview 2, Pos. 122). Another example, one notes that *“TikTok is a very big installed user base where producing video in large quantities (...)and people will just watch it regardless(...)”* (SG2–Interview 5, Pos. 97). However, like many other platforms, it does not provide access to its data (SG2–Interview 5, Pos. 97).

Moreover, platforms transmit data across borders, for example, Google’s data transfers involved *“12 companies with ‘Beijing’ in their names”* (SG2–Interview 3, Pos. 52). In this way, almost every voter is profiled by *‘unknowable parties’* (SG2–Interview 3, Pos. 52), with the lack of accountability on the part of platforms being the key problem. This concern links the issue to the generative AI market, pointing out that *“the generative AI market is based on data. Who controls all the data? The same three or four firms...”* (SG2–Interview 4, Pos. 285–287). Thus, it makes *“the system [is] vulnerable to disruption”* (SG2–Interview 3, Pos. 55).

In addition, a participant highlights that control over social media platforms has already been lost, and that the only remaining action is to establish the necessary guardrails for AI and other emerging technologies (SG1–Interview 4, Pos. 56). Another concern is that within a few years it may no longer be possible to distinguish what is authentic and what is not (SG3–Interview 2, Pos. 122). However, transparency mechanisms emerge as a key solution, directly linked to broader ethical themes such as transparency, accountability, and explainability. In particular, transparency would be a hope if people know who they are interacting with on platforms (SG2–Interview 5, Pos. 58).

Platforms differ greatly in their structure—some are open, others closed; some text-based, others heavily video or audio-based (SG1–Interview 5, Pos. 50). Yet, what is significant is the interconnected flow between platforms, from Facebook to YouTube, from TikTok to Telegram (SG1–Interview 5, Pos. 48). Despite this, no one fully understands how these platforms operate,

and the public must simply take the companies' words for it (SG1-Interview 5, Pos. 69). In this sense, this is a kind of black box, where debates proceed largely on assumptions (what ifs) and engaged in darkest imaginations (SG1-Interview 5, Pos. 69). However, interviewees are interacting with bots (SG1-Interview 3, Pos. 90), or to understand how long bot-generated content remains accessible on the platform (SG1- Interview 1, Pos. 50).

Thus, platform responsibilities may include actions such as *"taking down content in a timely manner"* (SG1- Interview 1, Pos. 50), providing *"transparency information about the ads they host"* (SG1-Interview 2, Pos. 62), implementing *"the labelling the watermarking"* (SG1-Interview 3, Pos. 90), and ensuring *"a certain degree of transparency or auditing in how platforms address bots and botnets."* (SG1-Interview 5, Pos. 56). However, platforms fail to act responsibly (SG2-Interview 3, Pos. 49).

The imbalance in regulatory enforcement encourages platforms to avoid taking responsibility. As a participant explains, platforms tend to treat the law as *"something that they need to actually pay any heed to beyond compliance theatre"* (SG2-Interview 3, Pos. 76-78). Thus, there is a preference to provide *'heavy regulation'* for platforms and even *a shift back* to how things used to be, though without resorting to outright censorship (SG3-Interview 3, Pos. 140-142). However, unlike traditional media, platforms do not have editors, and *"regulations are not based on freedom of speech. It's based on their own view of what they want on their platform"* (SG3-Interview 5, Pos. 71).

So, there is a growing demand for clarity about responsibility of platforms, specifically, who should be accountable for content shared through platforms (SG3-Interview 3, Pos. 127). Traditional media also supports this demand by targeting platforms when it suits them. As one participant explains: *"What made Cambridge Analytica so interesting for the traditional media was because they had a common enemy. That Facebook is the traditional media's enemy"*

(SG3–Interview 5, Pos. 72). Therefore, the power asymmetry, or struggle over power, is also visible between traditional media and new media.

In addition, this responsibility approach highlights the power asymmetry between rule makers and platforms. Participants frame platforms as a form of colonialism, which eliminates competition and leads to ‘*disastrous outcomes*’ for democratic processes (SG2–Interview 3, Pos. 76–78). This influence extends beyond the platforms themselves and can also be observed in regulatory processes. For instance, NGOs cooperate as expected with the public sector and with other NGOs (SG2–Interview 4, Pos. 260). At the same time, they raise the following question: “*How do we compete with the power of the fund?*” (SG2–Interview 4, Pos. 270–272). This is because is a persistent situation where commercial collaborators are always seen as more important than civil society and fundamental rights. Consequently, in the absence of better alternatives emerging regarding platforms’ responsibilities, surveillance, and manipulation become the only viable and sustainable model (SG2–Interview 3, Pos. 78).

As a result, participants emphasise the colonial position of platforms in eradicating competition. The lack of effective regulation, or enforcement difficulties on platforms, further reinforce this trajectory. Consequently, market dominance becomes increasingly consolidated in favour of platforms, and ultimately undermining democratic processes.

4.6.4. Ethics

The insights provided by participants on ethics were closely related to the previously discussed themes of democracy, media, and platforms. Ethical concerns were human-centred rather than technical. Participants emphasised that developers, deployers, and platforms must be responsible for their actions and services. Or, there is a grey zone to understand the responsibilities for algorithmic speech.

Therefore, ethical AI must involve accountable technological processes, tools, and operations provided through platforms. This accountable approach includes transparency as well, and participants also called for systematic auditing and transparency about bot removal or removing their functions. Therefore, transparency is required for three main reasons: (1) as a requirement for legal compliance, (2) in response to the “*black box*” nature of platform services, and (3) in relation to ethical principles needed for advertising. Also, transparency can be considered the most highlighted ethical principle across the participants.

In particular, without transparency about whether a user is interacting with a bot, the foundation of ethical political communication collapses. For instance a participant says “*We are talking about a black box, we don’t know what has happened. [There are] darkest imaginations about what we can do with these technologies.*” (SG1-Interview 5, Pos. 69). This means platforms should provide explainability, transparency and a trustworthy digital environment regarding their services and technologies.

On the other hand, scepticism about the adequacy of the legal framework was already discussed above. On legal compliance, participants reflect the strict approach to the necessity of ethical principles, underlining that transparency must be ensured in implementation. Because ethical requirements are only possible in a context where enforceable regulations exist, these themes cannot be considered separately from one another. However, it seems there are pressures within NGO–public sector cooperation: “*They felt unable to buy our services, as it were, to work with us for reasons of political neutrality.*” (SG2-Interview 5, Pos. 103). When NGOs become more active and engage directly in rights, ethical principles also seem to encounter a conflict: “*If we bring in rights protections, that’s probably going to need fewer jobs, because it means that the commercial model is interrupted or disrupted.*” (SG2-Interview 4, Pos. 270-272).

From political bots' perspective, bots are often not considered trustworthy (SG2-Interview 3, Pos. 29). For example, Interviewee 1 states: "When it comes to AI bots, there is the transparency requirement that the company or a political party must ensure when they're using AI bots." (SG1-Interview 1, Pos. 48 and supported by SG1-Interview 2, Pos. 51). Additionally, regarding advertising, all of the advertising activities, "accuracy, authenticity, legitimacy" should be the core principles. (SG1-Interview 5, Pos. 45).

From one participant's perspective, political campaigning work can still serve as a role even in non-democratic contexts: *"Even if it's [a country] far from what we consider as a democracy, we can help promote some kind of discourse in society between political leaders and the people."* (SG3-Interview 2, Pos. 110). This raises a critical question: can constructing a discourse to confer democratic legitimacy ever be considered ethical? Because elections are not only about winning, but about the ability to govern effectively, ethically. Thus, politicians themselves often lack this responsibility today (SG3-Interview 2, Pos. 116). It is disappointing that professional standards within the political campaigning industry are missing in terms of ethics. There is a different picture, highlighting not only internal company ethics but also the responsibility they feel during the campaign process itself, in particular, data, privacy, and standardisation. For instance, Interviewee 3 explains that they have designed a structure with accountability and responsibility in mind (SG3-Interview 3, Pos. 166-167).

From the private sector perspective, the participants' companies do not generally have an internally functioning ethical process. While a few share the need to establish one, overall, there is little interest in applying such processes within the company. For example, an interview explains that if a picture were to be modified in a political campaign, it would not be for deceptive purposes but only to make the image look better (SG3-Interview 1, Pos. 69). They find themselves responsible from this content and ready to explain it transparently (SG3-

Interview 1, Pos. 69). This reflects a valuable approach, almost like ethical political campaigning.

Therefore, participants are aware of the need for ethical requirements in politics, but questioned whether guidelines even existed or were widespread. The finding here is that guidelines on ethical sensitivities seem necessary for political campaigners or companies operating in this field (SG3-Interview 1, Pos. 71). Participants, in particular from SG3, shared that they had a duty to provide accurate information, which stemmed from their respect for European ethical standards. They added that things did not function the same way in the United States. In making this comparison, a participant explained that giving inaccurate views would harm society, and they were unwilling to take on such responsibility (SG3-Interview 5, Pos. 114).

For instance, a participant shared that they have been involved in different initiatives on political campaign ethics, trying to think of solutions and work toward them within an ethical framework (SG3-Interview 2, Pos. 90). In the ethics principles context, WIPO's ethical framework is considered a starting point (SG3-Interview 2, Pos. 90). Similarly, the European Association of Political Consultants' ethical principles (SG3-Interview 4, Pos. 244-249) and ESOMAR's ethical requirements are considered for services of these companies (SG3-Interview 5, Pos. 111-112). This shows that while internal processes may not exist, there is ethical awareness within companies, which is a valuable finding in this study. However, it points that professional standards were weak in this industry (SG3-Interview 5, Pos. 128-129).

4.6.5. Governance

In this thematic analysis, governance, as a main theme, reflects participants' approaches to the regulatory process of AI systems in the EU. Their explanations were not limited to the AI Act, but also referred to other EU regulations regarding AI systems, political bots, and their use in democratic processes. As one participant emphasised that the regulation has, perhaps surprisingly, prompted global reflection and debate on AI, and the participant put it: *"It's too early to say if it works. I think it certainly has people talking considering about the risk in AI. So if you wanted to talk, if you wanted to bring about a global conversation on AI that has definitely happened."* (SG2-Interview 4, Pos. 48-50). For this reason, these diverse perspectives are used to sub-categorise governance such as their general approaches, the challenges surrounding regulation and their underlying causes, the different expectations of the regulation, the varying views regarding the AI Act, and the participants' recommendations.

4.6.5.1. General Approaches of the Participants

In their general approaches, participants expressed a critical stance toward AI regulation, questioning its timeliness and appropriateness, while also demonstrating awareness of market dynamics and economic considerations. For instance, *"All these attempts at regulating something are sometimes a little bit lame, because they are lagging behind years and the technology development is so fast that once the regulation is out where a lot of work and the years of discussion has been invested, I mean the problem is already gone or maybe somewhere else. That's the one thing."* (SG3-Interview 2, Pos. 39). This perspective was supported by others. Another participant noted: *"These conversations that you hear legislators having about digital marketing, you're like, that would have been really helpful three years ago, but that's not where we are now, and the pace at which technology, technological developments*

happened, the pace at which AI is changing is so out of kilter with how legislators work.” (SG3-Interview 1, Pos. 40). On the other hand, another participant, who acknowledged from the outset that legislation will inevitably lag behind the rapid development of technology, expressed the following view: *“It's almost impossible for legislation to keep up. But I do think what we need to have in place are guardrails or basic principles around when it is appropriate to use AI, you know the ethical considerations around that.”* (SG1-Interview 4, Pos. 22).

One of the questions directed to interviewees was whether they believed AI could be regulated. In SG1, four participants were positive that AI systems could be regulated, with the exception of Interviewee 2. In SG2, four participants also believed in the possibility of regulation, except for Interviewee 5. In SG3, only two participants thought AI could be regulated, while three disagreed. Overall, this categorisation shows that roughly one in three participants did not believe AI could be regulated, and they provided various perspectives for this position. For example, some referred to negative experiences arising from earlier regulatory frameworks.

An example can be such as *“There's the suite of EU legislation recently is the Digital Services Act, is the really big one. Another one (...) is the European Media Freedom Act. There's also the revised audio Visual Services Directive and then now the AI Act (...). And there's a pattern where they start off talking really positively about democratic values and serving the interests of citizens. And then through this trilogue process and all the lobbying. They tend to be watered down quite a lot.”* (SG1-Interview 2, Pos. 22-23).

Some referred to the difficulties of achieving balance in online regulation as seen in earlier frameworks (Interviewee 5, Subgroup 2). An example can be *“I suppose that the only thing I can do is relate it to the other regulation that we followed. (SG2-Interview 5, Pos. 23)(...) The way I look, a lot of this like online regulation is like the balance, is to strike a very, very difficult and the risk of under regulating and over regulating a very, very great. (SG2-Interview 5, Pos.*

23).” Others argued that AI is more complex to regulate than is generally assumed. For instance, *“No, but it should. I think it's hard than people think.”* (SG3-Interview 5, Pos. 18).

One of the insights from this distribution is that disbelief in the possibility of regulating AI was most common among SG3, namely among professionals in private sector. The number is three out of five in SG3. Accordingly, an important question is whether the challenges emphasised by private sector participants, and which informed their disbelief in the possibility of regulation, were disregarded by participants in SG1 and SG2. This divergence in perspectives may, in fact, be closely related to the broader governance issues identified by participants, particularly those concerning balance of power and human’s role.

For instance, one participant noted: *“I think the problem that we see in all digital tech, and I'm sure AI is only even more so the case here, is that typically legislators and parliamentarians just ‘do not know the technology’, that the ecosystem of knowledge about how the technology works typically sits over here in private enterprise.”* (SG3-Interview 1, Pos. 40) Another participant in SG3 highlighted the role of humans, stating *“(.)so actually, I don't think it's basically regulations, it's more of a philosophical view on humans role in future that we have to work and work with more and the regulations should come second.”* (SG3-Interview 5, Pos. 18).

Notably, some participants approached AI governance through the lens of their awareness of global market dynamics and economic factors. This link between AI governance and market dynamics can, of course, be traced to the fact that the AI Act is product-based rather than human-rights-based. As one participant in SG2 supported this approach: *“It's also a product-based regulation. It's not based on human rights.”* (SG2-Interview 4, Pos. 39). Accordingly, market considerations were used by participants as a basis for drawing conclusions about the necessity of regulation.

For instance, *“AI is very much being developed in America, every man for himself. If you have all knowing generative AI and introduce it to Western job market, you will actually get riots in France, and you could get overregulation, (...) instead in France, they would completely banned AI because the farmers will hate you basically and that is more of a European perspective of how we see technology.”* (SG3-Interview 5, Pos. 18) After discussing the EU’s restrictive perspective, the same participant turns to China’s more controlling approach to AI governance, stating: *“China could have two different things, but they still have to feed their people. So it's very hard to understand how you have a billion people there that actually have to. And if you make them useless, then you are basically destroying the very foundation of how you control the people.”*(SG3-Interview 5, Pos. 18). Indeed, this perspective is quite interesting, as it highlights the socio-economic risks associated with the debated possibility of AI replacing humans.

From a liberal point of view, a participant suggested that, just as a regulatory pathway has gradually been found for digital currencies over the years, a similar approach could be developed for AI systems. as the participant explained: *“I think, like with the digital currencies... So when they came out, no one knew what to do about it. It is something new. There is no regulation. There is no framework. How do we regulate it? In years, we see that in the United States, they have found a way how to legalize that, and I think the same thing will happen with AI.”* (SG3-Interview 4, Pos. 170-171) From a more liberal perspective, the realisation that self-regulation, originally envisioned as a way of intervening in the market from ‘behind the curtain’ with minimal interference, has not worked appears to have led to increased regulatory measures. One participant explicitly emphasized this point: *“There is room for fundamental rights impact assessments, but they are not mandated. So they were supposed to obligatory. They are not. So there is an element of it, which is still self-regulation. Self-regulation, as we know, however, hasn't worked, and that's why they brought the DSA, that's*

why they brought the DMA, because they realised that the markets weren't working the way they needed to work. So it's too early to say if it works." (SG2-Interview 4, Pos. 44-48). In fact, as a result of self-regulation, a participant emphasized that relying on voluntary commitments of companies would not lead to meaningful outcomes, metaphorically describing such voluntarism as being *'like whipped cream'*. (SG1-Interview 3, Pos.35)

The awareness reflected by participants regarding the market is valuable in understanding the political economy of AI. This awareness relies on the future of AI and AI governance. Indeed, rather than continuing the debate on whether AI will replace humans solely through the lens of human skills and AI's capabilities, it becomes evident that focusing on the risks this competition poses for the state mechanism itself. At the same time, concerns arise over whether the EU's efforts and the significant resources invested, in regulating a technology largely developed in the United States may ultimately prove ineffective. Beyond the popularity of the EU's restrictive stance, the failure of self-regulation to function as intended emerges as a critical market-related critique, directly tied to broader questions of AI governance.

4.6.5.2. Challenges in the Regulation Process of the AI Act and Their Underlying Dynamics

During the interviews, many challenges highlighted by participants were related to the regulatory process of AI systems. The most shared views included power asymmetries, a lack of expertise in regulatory processes, and the complexity of the AI concept itself. These challenges are also the main sources of participants' concerns about the regulation of AI. The interviewees expressed doubts and apprehensions that, if these challenges are not addressed effectively, the regulatory process may result in completely useless legal tools. Additionally, the participants shared a common tendency to approach AI governance by referring to previous

regulatory frameworks in the EU, highlighting that AI poses significant risks. It seems there was a broad consensus on the relevance of adopting a risk-based approach to AI regulation. However, there was also a degree of disappointment stemming from the implementation of previous EU regulations.

A more detailed analysis reveals that there is an expectation for regulators to have sufficient expertise within the areas they regulate. This expectation also reflects broader inclusiveness of the regulation and the lack of representation of all segments of society in the regulatory process. It is particularly noted that knowledge about how the digital ecosystem functions is largely held by the private sector, which is perceived as being less transparent (SG3-Interview 1, Pos. 40). As highlighted by the same participant, companies are often reluctant to give away any business advantage by speaking publicly about how their technology works (SG3-Interview 1, Pos. 40).

Furthermore, the involvement of platforms or big tech companies in the regulatory process is seen as one of the reasons why the approach of AI Act was product-based rather than human-rights-based (SG2-Interview 4, Pos. 39). At the same time, lobbying activities were described as having “watered down” the regulatory process, raising further questions about the extent to which the final version of the AI Act was influenced by these lobbying activities (SG1-Interview 2, Pos. 23).

As a result, even though the AI Act is a market-based regulation, it must still prioritise public interests. It seems the imbalance remains significant when compared to private sector in terms of experts in AI. As private sector employs a larger number of experts across diverse fields, this creates a persistent power asymmetry in expertise for public sector. For instance, it is difficult for a public-sector expert in regulatory process to receive the same level of compensation and benefits as an expert working for a big tech company. This asymmetry relies on responsible use of limited public resources, whereas companies may allocate funding where

profitability is possible. The accountability constraints do not work the same in public institutions and private sector. These structural differences recreate one of the challenges surrounding AI Act.

4.6.6. Discussion

In this section, the interviews are analysed under five main themes which are AI systems, bots, democracy, ethics, and governance. The aim is to provide an analysis and discussion of how the findings derived from these themes may influence the current legal framework. These analyses also offer preliminary insights that inform the recommendations presented in the conclusion, in Chapter 5.

Accordingly, there is no clear consensus among participants regarding their understanding of AI systems or of AI more broadly. Each participant tended to focus on a different aspect or dimension of AI. As a result, this theme reflects the diversity of professional perspectives within this field.

The interviews present a shared concern across public, private, and civil society sectors regarding the use of political bots and their broader implications for democracy. While participants shared diverse definitions of AI, many participants agreed on the view that political bots function as manipulative actors. Namely, political bots amplify disinformation and reshape public opinion. As a result, political bots can be used for distorting democratic discourse.

It seems that the concept of the bot, as a theme, reflects how participants conceptualised bots by grounding their descriptions in everyday experiences, practices, and interactions. This theme addressed participants' general descriptions, knowledge, and perspectives about bots alongside their views on the use of political bots in the public sphere and the effectiveness of

the existing legal framework for bots. Participants tended to respond to the questions from a democratic framework, frequently highlighting the negative characteristics and aspects of bots.

The insights regarding the use of political bots also brought forward other interrelated themes, including democracy, the media environment, media ecosystem and ethics. Many participants were confident that bots would become increasingly widespread in the future. The overall discussion suggested that debates surrounding bots are ongoing and will likely expand as more advanced and complex forms of bots emerge across various sectors. Additionally, each sector perceives and engages with bots differently, however, all approached them with caution. Interestingly, this cautious approach seems quite conservative in the digital era when bots are often perceived as revolutionary technologies. Thus, when even AI professionals themselves express such caution, there would be an important question: Does regulating these widely used tools within a still fragmented legal framework underestimate their potential impact?

From a political perspective, interviewees highlighted the ethical requirement of transparency and accountability, especially during democratic processes. However, the responsible actors did not mention it. Notably, no participant voiced a clear position on platform responsibilities. At the same time, participants were aware of the regulatory ambiguities about bot speech, as well as the absence of clearly defined responsible actors. As a result, the most significant ethical issue identified by participants was the need for transparency in bot–user interactions, namely, that users should be clearly informed when they are engaging with a bot.

Additionally, these requests seem abstract and need to be located in a concrete framework. For instance, transparency would not be thinking without explainability. Social media was seen as vulnerable to bot-driven narratives; in contrast, traditional media appeared to remain a more trusted source for the public. However, current legal frameworks were widely considered to be inadequate in addressing the scale and speed of these technologies. Participants called for

adaptive governance models that combine enforceable regulation. They also emphasise the importance of cultural, normative, and public engagement to protect democratic values in an AI-driven political information ecosystem.

Consequently, this highlights the need to develop a framework of political ethics suitable for the age of AI. Although a few participants highlighted the potential positive uses of political bots in democratic processes, such voices remained relatively limited across the interviews. While participants appeared aware of the risks, the complex nature of the issue led to diverse focal points within their responses.

On the other hand, regarding the ethical use of AI were relatively limited in the analysis. However, a key finding emerged from private sector participants: despite holding administrative roles, they confirmed that their organisations have no internal mechanisms to ensure the ethical use of AI. The absence of such internal ethical processes and principles among companies that participate in or advise political campaigns represents a crucial governance gap. Ultimately, ethical principles should be considered essential, particularly for companies and political actors involved in political campaigning. Moreover, political parties should integrate technology ethics into their party programmes and strategic frameworks. This is a core moral responsibility in the digital age for democracy.

Insights on governance showed that different sectors involved in the regulatory process may not be working in full cooperation and communication. For example, the positive reflections of NGO employees on the regulation of AI systems were not observed in other groups. In particular, even though the participants in SG3 value face-to-face political communication, SG1 and SG2 seemed unaware of the specific risks posed by political bots identified by the industry. For these reasons, there are blockages in the rulemaking process, and these are not only procedural. They also make intensified cooperation and communication a necessity.

There is still uncertainty about whether new technologies can be regulated in time. Two common examples were raised: (1) the disappointments around GDPR enforcement, especially enforcement difficulties for platforms, and (2) the amendments in draft AI Act for GPAI. This suggests that expectations related to the AI Act already lag behind technological developments. At the same time, participants pointed out that regulatory processes are too important to be left to non-expert politicians.

Indeed, there is a common concern that the negative experiences associated with the GDPR may reoccur in both current and future technology regulations. This apprehension relies on the perception that the GDPR's implementation process, though well-structured, organised, and rights-based in theory, has not functioned effectively in practice. As a result, participants viewed the AI Act with a certain degree of scepticism, emphasising similar shortcomings. Interestingly, all three interview groups tended to focus on different dimensions of both the regulatory process and AI systems themselves. The insights show that because of the lack of cooperation and collaboration among these sectors, implementation will not be effective for the AI Act. Then, the shared fear that the AI Act may mirror the similar implementation challenges of the GDPR appears almost as a self-fulfilling prophecy.

Of course, the involvement of commercial actors in the entire regulatory process, combined with their unlimited resources compared to public authorities, clearly shifts the balance of power in favour of tech companies. This appears to be a complex and central issue that warrants further examination from a governance perspective in future research. The insights show that there is a clear imbalance emerges when the limited and planned public resources for regulatory processes, such as budgets, labour capacity, and time, are compared with the vast financial and technological capacities of corporate actors. Also, at this point, concepts such as lobbying and power asymmetry enter as new codes on MAXQDA. However, these are not fully explored,

since all participants did not consistently responded from these perspectives. In addition, the most significant concern expressed was that politicians lack sufficient knowledge about AI and technology to participate effectively in the rulemaking process. This finding derives from the participants' questioning whether the level of expertise in AI technology among politicians and their rapporteurs is sufficient to enable comprehensive regulation. As a result, the findings clearly demonstrate a broader sense of concern and even a lack of confidence in regulatory processes.

On the other hand, the impact of new media is important to highlight. As discussed in Chapter 2, where Habermas pointed to platforms' tendency of avoiding responsibilities, these concerns are echoed in this research. Participants highlighted the ethical requirements, in particular transparency. For new media, participants reflected that elections cannot be won solely by using new media. Traditional media, especially television, remains the most important electoral tool. This is both surprising and, at the same time, a sign of democracy's resilience against technological speed. In this context, one of the supposed positive uses of bots, reaching voters cheaply and quickly, seems to lose its meaning. Even minor parties, who might see this as an advantage, appear unable to winning elections through such strategies. Additionally, developing ethical principles for political campaigns appears necessary within a perspective that prioritises technological tools.

At the same time, the theme of democracy under threat emerged almost as a consensus. Yet this was never stated explicitly. Instead, concerns were expressed through other concepts such as, political bots, manipulation, the widespread use of social media, or the rise of the far-right in other countries. But no participant showed the platforms as responsible actors. The same applies to platform responsibilities as well. Although there is a clear grey area here, none of the participants directly stated that platforms must be held accountable. Although AI literacy

was rarely mentioned in these insights, it still seems to be one of the best possible solutions against manipulation and toward building a well-informed society.

Therefore, the findings of this study point toward many other concepts that could be explored further. The research does not ignore the threats to democracy, but also reflects a recognition that the perceived danger might, to some extent, be overstated. For example, one important finding is that elections cannot be won by political bots alone.

Yet in highly polarised societies, where electoral strategies are designed with extreme precision, this does not rule out the possibility that bot could still influence election results. Finally, the inability to measure the influence of political bots makes it impossible to fully validate the findings of this study with respect to bots alone.

4.6.7. Future Research

The findings of this study provide implications for the direction of future research. This study employed socio-legal research approach and thus enables examination of the influences and use of political bots in democratic processes from both social and legal perspectives. Additional insights could be gained by conducting similar qualitative studies involving participants from non-EU countries. This would allow the research findings to be extended beyond regional boundaries.

Future research could focus on exploring and discussing the findings of this research in relation to other EU regulations that can be applicable to political campaigns, democratic processes and technological tools. For instance, focus groups and semi- structured interviews could be conducted with a larger number of participants to further explore the findings. This would not be with the intention to verify the findings of this research, but rather to further explore and

discuss how other EU regulations might be applied to political bots and their implications for freedom of expression and information.

On the other hand, the findings of this research have potential for wider use. The findings conclude with specific recommendations in this research, but they could support policy-making efforts at EU or national levels. Accordingly, the limitations of this research provide scope for future academic research. In other words, the insights gained in a more transparent AI industry ecosystem may be more valuable for future research.

4.7. Conclusion

This study highlights both the points of consensus and differences across sectors regarding the legal framework of political bots. The primary aim of the research is to identify cross-sectoral perspectives on political bot regulation and to generate findings that contribute to the development of a more effective and adequate regulatory framework. Despite differences in how participants defined AI, there was a shared understanding that political bots amplify disinformation, simulate consensus, and distort democratic discourse. The findings highlight the ethical importance of transparency and accountability, especially in political contexts. Accordingly, traditional media continues to be considered as more trustworthy compared to social media, which is seen as more vulnerable to AI bot-driven manipulation. However, current regulatory frameworks are widely seen as inadequate. Participants called for adaptive governance models, thus, it is possible to combine legal enforcement with societal and cultural engagement to address emerging risks in AI-driven political communication.

Overall, this chapter in thesis analysed interviews conducted with AI professionals through thematic analysis using MAXQDA. It presented the main insights and findings of the empirical research. Accordingly, Chapter 4 provides empirical findings derived from interview data.

However, these findings are not intended to directly test or verify the theoretical and legal arguments developed in Chapters 2 and 3. Rather, the interview data aim to complement and expand the conceptual and legal discussions developed in the previous chapters. Therefore, theoretical, legal, and empirical findings are concluded in next chapter of the thesis, in Chapter 5. The final chapter develops the key conclusions of the research together with policy recommendations at both national and international levels. In addition, the limitations of the thesis and suggestions for future research are also discussed in next chapter, Chapter 5.

Chapter 5: Conclusion

5.1. Introduction

This thesis has examined whether the AI Act provides a legal framework for political bots. Research claims that individuals were directed or manipulated by generative AI-driven political bots during the elections.⁶⁶³ They were employed in referendums such as Brexit referendum and the Catalan independence referendum.⁶⁶⁴ They were also used in elections in many countries, including EU member states, where they influenced election results.⁶⁶⁵ So, the research was structured around two core research questions: How are political bots used as tools for manipulation in political elections in Europe; and how could the EU's AI Act prevent political bots from being used as tools for manipulation without interfering with pluralism and freedom of expression and information? To enable these compact responses to the research questions, this thesis adopted a socio-legal research methodology and conducted interviews with professionals in AI, as well as law-in-context analysis of the AI Act and relevant documents from the EU legal framework. For the interviews, open-ended questions were chosen, and semi-structured interviews were conducted. The gathered data was analysed by using MAXQDA software and applying thematic analysis.

This thesis was divided into six parts in order to address two research questions. The first chapter examined introduces what bots are and provides a short overview of the problems they

⁶⁶³ Simona Bader and Lucian-Vasile Szabo, 'Voter Manipulation and Electoral Campaign Hijacking by Social Media Technologies. The Romania 2024 Case' (2025) <<https://doi.org/10.2139/ssrn.5243802>> accessed 4 June 2025.

⁶⁶⁴ Bello and Heckel (n 11); Bessi and Ferrara (n 17); Stella, Ferrara and De Domenico (n 126).

⁶⁶⁵ Aneta Zachová (n 26); Federal Foreign Office (n 25); Fernquist and others (n 30); Ferrara, 'Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election' (n 31).

pose for democratic processes, both in the literature and in practice. It offered a concise overview of the structure of the thesis. The second chapter provided a theoretical framework and address AI governance for political bots. The theoretical framework relied on Habermas's public sphere theory, as political bots operate primarily within the political public sphere. Thirdly, the research presented legal framework for political bots by addressing AI Act, Article 11, Article 7 and Article 8 of the CFR. In Chapter 1, the methodological framework was presented and the reasons for the methodologies adopted in this thesis were explained. This chapter functioned as a bridge to Chapter 4, which presented the interview findings and explores whether the theoretical and legal frameworks developed in Chapters 2 and 3 correspond to practical expectations.

This chapter, Chapter 5, provided the reader with an evaluation of the design and methodology of the thesis as a whole. This final conclusion chapter presents a summary of the findings, as well as the key conclusions and recommendations that emerged from them. Further, the chapter discuss the overall significance, limitations and implications of the thesis. Then, the chapter concludes the thesis by outlining the key conclusions, presenting concrete practical recommendations, and proposing areas for future research.

5.2. Research Overview

This research aimed to provide a socio-legal analysis of the potential influence of the EU's AI Act on political bots from the perspective of freedom of expression and information, as articulated in Article 11 of the CFR. In line with this objective, the thesis has sought to answer two core research questions: How are political bots used as tools for manipulation in political elections in Europe; and how could the EU's AI Act prevent political bots from being used as tools for manipulation without interfering with pluralism and freedom of expression and

information? Accordingly, political bots are strengthening by generative AI models, advanced technologies that facilitate the spread of disinformation. Yet, their functions are not limited to disinformation. They are also deployed to create echo chambers, to silence or marginalise candidates or their supporters through targeted strategies, such as manipulative interactions, amplification of polarisation, or coordinated online political harassment. Also, political bots exploit grey areas within the EU legal framework. These grey zones are also recognised and utilised by the platforms. From the perspective of public sphere theory, political bots can be understood as operating within these platforms, that is, within the digital political public sphere. They pose significant systematic risks and require FRIA. For this purpose, the expectations and potential risks concerning a risk-based framework and an integrated risk culture in society, as well as the assessments, are provided in Chapter 3.

The AI Act does not explicitly promise to regulate political bots, but it provides a regulatory framework that could apply to them. However, the current legal framework it falls short of expectations, largely due to the complexity and lack of clarity of the AI Act. Moreover, the absence of a specific regulatory framework for addressing the algorithmic speech generated by political bots further deepens the legal gap in this area. To close this legal gap three approaches can be applied from the perspective of political bots. First, the AI Act should establish a clearer framework that especially highlights the reasons for regulating democratic processes in a product based regulation. The Act should also articulate clarity regarding its relation to fundamental rights and the broader transformation of democracy and democratic process in the digital age. By doing this, the AI Act should not reduce political bots and AI systems used in democratic processes merely to tools of disinformation. Instead, it must recognise the broader democratic implications of their use. Second, the AI Act links primarily to the right to vote under Article 39 of the CFR and in Recital 62. However, this narrow focus limits its ability to

comprehensively address the full complexity of democratic processes. Instead of focusing on this limited connection, the right to stand for elections should be emphasised, as it is equally inherent to the concept of a truly democratic regime. Third, and in line with Habermas's public sphere theory, the regulation should aim at avoiding excessive fragmentation of the political public sphere. A more coherent and trustworthy digital public sphere will ensure pluralism and democratic deliberation.

On the other hand, the significance of this research can be identified in several dimensions. First, it is likely to be one of the first studies to address "democratic processes" within the high-risk AI systems category under the AI Act from the perspective of political bots.⁶⁶⁶ In addition, by examining the relationship between political bots and the right to freedom of expression and information as articulated in Article 11 of the CFR, the study expands its legal framework to include the CFR.⁶⁶⁷

The second, this research contributes to multiple interdisciplinary fields, including AI law, sociology, media studies, election law, and constitutional law, by contributing a multidimensional analysis. By adopting Habermas's public sphere theory, the research positions political bots within that theoretical framework, thereby providing a legal perspective that enriches the fields of sociology, political communication, and media studies.

Furthermore, the study also presents novelty within its theoretical framework. This is because the research examines both the concept of the public sphere and political bots within a new legal field, that of AI law and the AI Act, through the lens of Habermas's revised views on the

⁶⁶⁶ Artificial Intelligence Act (n 40) app III.

⁶⁶⁷ Charter of Fundamental Rights of the European Union (n 39) art 11.

public sphere theory.⁶⁶⁸ On the other hand, this research fills a critical gap in AI law. It approaches AI law from a public law perspective, providing insights from the viewpoints of democracy, elections, and constitutional law.

As an interdisciplinary study, multiple research methodologies were employed, namely socio-legal research methodology and qualitative research methodology. These methodological approaches allowed flexibility and enabled the application of various research methods, such as law-in-context analysis, interviews, and thematic analysis. As a result, the insights derived from these distinct approaches enriched the study's findings, diversified its recommendations, and strengthened its conclusions. The methodological diversity also ensured that the research did not repeat the existing literature or common views, resulting in an original and distinctive contribution. Therefore, this research presents an original, timely, and novel contribution to the existing literature by integrating its legal findings with insights gathered from interviews.

5.3. Limitations

Despite its originality, this research has two main limitations. First, this study was conducted over a dynamic period that began when the draft of the AI Act was first published on 21 April 2021 and continued until its official publication on 12 July 2024 in the Official Journal of the European Union. The dynamic nature of this timeline occasionally limited the research. This was because the regulation remained in draft form for a long time (relatively long time for this research period was only 4 years) and had frequent amendments and additions before its final version was adopted. Moreover, emerging debates⁶⁶⁹ and technological developments, such as

⁶⁶⁸ Habermas (n 145).

⁶⁶⁹ Hadrien Pouget and Ranj Zuhdi, 'AI and Product Safety Standards Under the EU AI Act' *Carnegie Europe* <<https://carnegieendowment.org/2024/03/05/ai-and-product-safety-standards-under-eu-ai-act-pub-91870>>; Natali Helberger and Nicholas Diakopoulos, 'ChatGPT and the AI Act' (2023) 12 *Internet Policy Review* <<https://policyreview.info/essay/chatgpt-and-ai-act>> accessed 31 March 2023; Moritz Lauer, Andrea Renda and Timothy Yeung, 'Clarifying the Costs for the EU's AI Act' [2021] *Centre for European Policy Studies (CEPS)*

the so-called “ChatGPT revolution,”⁶⁷⁰ also influenced the focus of the regulation during this period.⁶⁷¹ These ongoing changes sometimes shifted the regulation’s focus, which required sustained effort to maintain the research’s focus on its core research questions and protect it from the uncertainty surrounding the AI Act. Second, there were overlapping regulatory frameworks, such as the DSA⁶⁷² and TTPA,⁶⁷³ that occasionally influenced the focus of this research. Nevertheless, the study remained within the boundaries of the framework defined by the AI Act and its guidelines.⁶⁷⁴

5.4. Key Conclusions, Recommendations, and Future Research

The following section will briefly outline the findings of this research. These conclusions are structured to summarise the main insights drawn from Chapter 2, which presented the theoretical framework, Chapter 3, which examined the legal framework, and Chapter 4, which analysed the findings derived from the interviews. The section also provides recommendations for policymakers and highlights areas for future research that could contribute to the literature.

<<https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/>>; Jeremy Fleming-Jones, ‘EU AI Act Nearing Agreement despite Three Key Roadblocks – Co-Rapporteur’ [2023] *Euronews* <<https://www.euronews.com/next/2023/10/23/eu-ai-act-nearing-agreement-despite-three-key-roadblocks-co-rapporteur>>.

⁶⁷⁰ Bassini (n 161) 376.

⁶⁷¹ For instance, on 21 February 2024, the European Artificial Intelligence Office was launched within the Commission under the Directorate-General for Communication Networks, Content and Technology, to support the implementation of the AI Act, particularly regarding general-purpose AI.

⁶⁷² Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (n 167).

⁶⁷³ Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (n 41).

⁶⁷⁴ ‘The General-Purpose AI Code of Practice’ (n 477); ‘Code of Practice for General-Purpose AI Models’ (n 475); ‘Commission Guidelines on the Definition of an Artificial Intelligence System Established by Regulation (EU) 2024/1689 (AI Act)’; ‘Approval of the Content of the Draft Communication from the Commission - Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)’.

5.4.1. Key Conclusions

In exploring political bots, this research addressed three interconnected dimensions: democratic resilience, sustainable elections, and AI governance for political bots. First, democratic resilience via digital tools was discussed, emphasising that sustaining democracy requires engaging both political theory and legal frameworks. Second, sustainable elections were analysed through the intersection of electoral law and digital technology regulations, in particular the AI Act, aiming to highlight how legal and technological frameworks mutually reinforce democratic sustainability. Finally, the AI governance for political bots highlighted the importance of legal flexibility and future adaptability, recommending that regulations remain effective amidst continuous technological innovation.

For understanding democratic resilience, Habermas's public sphere theory provided valuable insights in Chapter 2 for this study. Habermas argued that the boundaries between the public and private spheres are becoming increasingly blurred. Building on this, this thesis advances the claim that, whereas Habermas described the public sphere as historically deriving from the private, in the age of AI, the dynamic appears reversed: the private sphere must now make deliberate and effective efforts to defend itself from being eroded by the public sphere.

Furthermore, political bots operating on digital platforms are strengthened by platform algorithms. Thus, the thesis highlights that the central challenge emerges from the absence of transparency within the platforms, and in the end, the platforms' tendency to avoid responsibility as Habermas highlighted in his later reassessment of the public sphere theory. Furthermore, several interviewees expressed views that, while expressed from different dimensions and perspectives, parallel Habermas's insights; these findings are examined in detail in Chapter 4. Yet transparency and responsibility alone are not sufficient: only when

combined with accountability and embedded in a trustworthy ecosystem can they offer meaningful safeguards.

From a legal perspective on democratic resilience, Chapter 3 first examined whether political bots fall within the scope of the AI Act. It was established that they qualify as AI systems. The next step evaluated where political bots are situated within the risk categorisation system of the AI Act. It becomes clear that, although political bots may rely on relatively simple technologies, they are nonetheless classified as high-risk systems. This is because they are designed to interact with individuals in democratic processes for political purposes.

However, two uncertainties remain at this point: first, what exactly is to be understood by “democratic processes”; and second, the undefined timeline of such processes. Both require clarification in the Act. Moreover, the risk categorisation system under the AI Act brings with it numerous exceptions. For instance, AI systems used to optimise, organise, or structure political campaigns are not considered in high-risk category. Political bots, however, could exploit this exemption by collecting data or being deployed in campaign structuring.

Political bots may also benefit from the capabilities of GPAI which makes them more functional as advanced versions of chatbots. Thus, systemic risk analysis and the application of FRIA are required for political bots. Although the GPAI Code of Practice seeks to provide clarity in systemic risk assessment procedures, such clarity is largely absent in the context of political bots.

In addition, the AI Act, as a product-based regulation, regulates AI systems used in democratic processes. This means that such processes are treated as business activities, and the use of AI

systems within democratic processes is accepted as part of a business model. The structural approach established by the AI Act does not align with the existence of democracy as an ideal. From the perspective of political philosophy, this indicates that democracy itself is increasingly reduced to a matter of marketing. In doing so, the EU effectively endorses the design of a new era in which democratic ideals are transformed into market-oriented practices.

For the assessment of political bots and freedom of expression, it seems the evaluation of algorithmic speech has not been widely explored within the EU's legal framework. As a result, it has not yet been prioritised in regulation. Algorithmic speech therefore remains in a grey area. The harm caused by political bots is collective rather than individual, eroding both democratic processes and democratic society as a whole. Thus, political bots cannot be addressed within the framework of Article 22 GDPR. Under Articles 7 and 8 of the CFR, however, responsibility must be considered, since political bots gather and use personal data. This responsibility must also be connected to Article 11, as the activities of political bots are ultimately a form of algorithmic speech. Additionally, political bots and computational politics represent, in effect, a business version of fundamental rights violations: (1) infringing the principle of the secret ballot, (2) undermining the effect of the free ballot, and (3) at times restricting individuals' freedom of expression. In this way, they violate the individual right to the privacy of personal belief.

For the governance of political bots, it seems that the globalist-era concept of "governance," which was meant to replace "government," has failed due to the absence of effective and ready-to-implement regulation of AI systems. The first reason is that even though the EU legally positioned itself as the primary actor of rulemaking, the process ultimately stalls at the level of implementation because of the self-governance concept. The second reason is that the actors

involved in the rulemaking process have, in practice, only reinforced oligopolistic control over most digital information and communication infrastructures, systems, and processes. In this sense, the third reason, the failure of “governance” reflects not merely a practical limitation, but the inherently anti-democratic character of the governance initiative itself.

On the other hand, the findings from the interviews, which are analysed in detail in Chapter 4, constitute an important foundation for the policy recommendations on sustainable elections developed as an outcome of this research. Accordingly, there appeared to be no clear consensus among participants regarding their understanding of AI systems or of AI more broadly. This shows that AI remains a complex concept on which consensus is difficult to achieve, even among professionals working in this field. Therefore, this finding suggests that regulating AI systems poses a significant challenge.

There is a general tendency to be cautious about bots. The overall discussion shows that debates surrounding bots are ongoing and will likely expand as more advanced and complex forms of bots emerge across various sectors. Interestingly, this cautious approach may appear conservative in an era when bots are often perceived as revolutionary technologies. Thus, when even AI professionals themselves express such caution, it raises an important question: Does regulating these widely used tools within a still fragmented legal framework underestimate their potential impact?

In addition, there is a tendency to address any negatively perceived situation through more regulation. Participants tended to conceptualise bots by frequently highlighting their negative characteristics and aspects. In doing so, they reflected a broader trend for regulating bots and, consequently, expanding regulatory measures. Thus, the issue of overregulation, both raised

by participants themselves and discussed in the literature, appears to be ignored when it comes to political bots.

Regarding the regulatory process, when examined through the lens of political bots, the AI Act acquires a political and economic dimension, as it also regulates democratic processes. There are two main conclusions drawn from this analysis. First, the most significant concern expressed was that politicians lack sufficient knowledge of AI and technology to participate effectively in the rule-making process. The research also highlights the lack of cooperation and collaboration among the public sector, the private sector and NGOs. This research concludes that the level of expertise in AI technology among the actors involved in the regulatory process remains questionable.

Second, the shared fear that the AI Act may mirror the outcome of the GDPR appears almost as a self-fulfilling prophecy. This is because the broad concern about the negative experiences associated with the GDPR may reoccur in both current and future technology regulations. Thus, the research concludes that there is a broader sense of concern and even a lack of confidence in regulatory processes. Additionally, as mentioned above, it was highlighted that the AI Act remains “a very complex law” and may still contain “loopholes” (SG2-Interview 2, Pos. 95). These observations suggest that the current regulatory framework may require further clarification, simplification, and adaptive revision mechanisms.

From political ethics perspective, the transparency of bot interactions emerged as a prominent issue. However, transparency alone is not sufficient. In addition to informing users that they are interacting with a bot, there must also be explainable information about how the bot is able

to interact with users. Ultimately, this research brought the necessity of moral responsibilities and digital ethics principles in political campaigning to the forefront.

This research also concluded that the use of public resources to regulate platforms is not sustainable. There are ongoing discussions about lobbying activities in relation to the power asymmetries between governments and platforms.⁶⁷⁵ Insights highlighted that the EU has been affected by power asymmetries because of lobbying activities. This raises the complexity of public resource issue. Accordingly, there is a clear imbalance emerges when the limited and planned public resources (including budgets, labour capacity, and time) are compared with the vast financial and technological capacities of corporate actors. This imbalance reflects not just a power asymmetry but a form of corporate colonialism that may ultimately absorb the functions inherent to the state itself. As a result, this imbalance ultimately poses a risk to the integrity and cohesion of the Union itself.

5.4.2. Recommendations

This section outlines five main recommendations derived from the research. These recommendations address both legal and governance aspects of political bots and AI regulation. They focus on building a well-informed society, clarifying the legal gap concerning the speech of political bots, promoting a more participatory regulatory model, ensuring that platforms maintain a balance between freedom of expression and responsibility, and supporting transparency to ensure public trust in rulemaking processes. These recommendations are explained below.

⁶⁷⁵ Pascale Davies, 'The New EU AI Act Is under Threat from Lobbyists, Experts and the Public Agree' [2023] *Euronews* <<https://www.euronews.com/next/2023/11/29/europes-ai-act-under-threat-by-lobbyists-experts-and-the-public-say>>.

Drawing on Habermas's public sphere theory, although the ideal of a well-informed society may seem difficult to achieve,⁶⁷⁶ it should, in fact, be possible in the post-broadcast age.⁶⁷⁷ Concretely, this can be realised through political parties' adoption of digital ethics principles and the integration of digital ethics approaches into their party programmes. In addition, governments and platforms can contribute to a well-informed society by making use of related EU legal tools, such as DSA and TTPA alongside the AI Act. Thus, political campaigning processes can be conducted consistently with the digital age.

For this purpose, the existing legal gap about algorithmic speech can be addressed through the implementation of current legal frameworks. This is because the regulatory gap concerning political bots is closely linked to the implementation process of the AI Act. This research does not recommend more regulations for the field. Effective implementation of existing regulations depends on to avoid overregulation. Instead, this research concludes that judicial interpretations can play a key role in filling this gap.

Freedom of information includes both access to information and the provision of information. Therefore, while regulating disinformation, deepfakes, and similar risks, lawmakers should not overlook media pluralism as a core element of democracy. In this regard, legal frameworks could focus more clearly on defining the criteria expected from information itself. The law needs to define and describe the information; further, it needs to answer legally what the information is. Such an approach may help address disinformation-related risks while also preserving media pluralism against manipulative bot activities.

⁶⁷⁶ Culloty and Suiter (n 215).

⁶⁷⁷ Lawrence Lessig, 'Rendering Sensible Salient' (2018) 27 *The Good Society* 171 <<https://doi.org/10.5325/goodsociety.27.1-2.0171>>.

In addition, the primary policy priority should be to ensure open communication and collaboration among governments, academia, NGOs, and politicians. Interview data also revealed structural tensions within governance and regulatory processes. Interview data also revealed structural tensions within governance and regulatory processes. NGOs are generally expected to cooperate with public authorities and other civil society actors. However, the one participant questioned: “How do we compete with the power of the fund?” (SG2-Interview 4, Pos. 270–272). In rulemaking processes, relevant actors, such as government representations, NGO workers, and other participants from the public sector need to collaborate on equal terms. The main purpose should be to protect the interests of society. Instead, the research revealed that in practice, regulatory processes may themselves reproduce existing power asymmetries between commercial actors, NGOs, governments, and other stakeholders.

Accordingly, policy recommendations should also aim to ensure more balanced participation conditions within regulatory and governance processes. In particular, stronger institutional and financial protections for NGOs and civil society actors may be necessary to enable them to raise concerns and participate independently in AI governance discussions. NGOs should be institutionally and financially strengthened within AI governance processes. Because NGOs may function as dynamic bridges between society and lawmakers. Due to their more flexible, active, and socially embedded structures, they may often remain closer to communities than state institutions. Also, this may help them communicate societal concerns to lawmakers more effectively. Financial independence may also encourage NGOs to act more freely in the public interest. In addition, NGOs may contribute to raising public awareness regarding AI-related democratic risks.

The focus should thus not be on introducing new regulations but on improving the implementation of existing ones as mentioned above. To enhance cooperation, more inclusive models, such as hybrid models, digital deliberative polls could be adopted.⁶⁷⁸ This may also help NGOs act more independently from financial dependency pressures, as mentioned above (SG2-Interview 4, Pos. 270–272), enabling them to defend public interests and voice their concerns more openly. Thus, these models could facilitate participation and collaboration among different actors during both the drafting and implementation phases of regulation.

Such a system would allow potential problems related to political bots to be observed. NGOs working in this field are already aware of the activities of political bots during election periods; moreover, industry actors can provide informed insights into the purposes, frequency, and strategic use of political bots in campaigns. In parallel, academic studies focusing on bot detection and research on the prevalence and intensity of political bot usage already exist.⁶⁷⁹ Politicians, in turn, can concentrate on how to regulate these systems effectively in the future, if necessary. Thus, reflections from all actors can contribute to the development of a stable, inclusive, and participatory risk framework for political bots. Moreover, concerns about the lack of expert knowledge among politicians and other rulemaking actors could be reduced, thereby, contributing to trust-building within society. Through such collaboration, implementation stakeholders would provide expert feedback, which would be both valuable and practically feasible. This approach could enable national authorities and Member States to meet the broad, complex, and high expectations associated with the AI Act at the national level.

⁶⁷⁸ *ibid* 174.

⁶⁷⁹ Rodríguez-Ruiz and others (n 112); Rauchfleisch and Kaiser (n 374); Yener, Najafi and Varol (n 513).

On the other hand, concerns about democracy must not be reduced merely to disinformation or deepfakes, but rather understood within a broader democratic framework that recognises democracy as a structural and evolving system. A forward-looking action plan should therefore be developed; one that anticipates the potential challenges of 2050, rather than reacting only to those of 2026.⁶⁸⁰ Such a plan must be designed through supranational cooperation, reflecting the shared democratic responsibilities that transcend national borders.

As for the platforms, conventional methods such as content removal or filtering may risk compromising freedom of expression for the sake of corporate profit. Therefore, platforms should revisit their policies while adhering to the early internet's promise of openness and freedom, aligning their future actions with governmental objectives. Additionally, the distrust created by lobbying activities within AI governance seems to overshadow expectations from regulation. Therefore, implementing more transparent regulatory processes, through enhanced communication and collaboration, would be essential to rebuilding trust and ensuring effective AI governance.

5.4.3.Future Research

Future research could further investigate how the implementation of the AI Act influences the legal and ethical responsibilities related to political bots. Since this study was conducted before the AI Act was fully implemented, future research should revisit this topic once the legislation is in effect. Analysing how concrete approaches, such as codes of conduct and guidelines regarding the implementation of the AI Act, shape responsibilities for developers and platforms would deepen the understanding of compliance challenges and evolving legal interpretations

⁶⁸⁰ Samuel Woolley and Dean Jackson, 'We Research AI Election Threats. Here's What We Need to Prepare for' *The Guardian* (9 October 2025) <<https://www.theguardian.com/commentisfree/2025/oct/09/artificial-intelligence-research-election-threats>>.

in AI governance. This could also clarify how uncertainty during the pre-legislative phase, which this research has partially reflected, influenced earlier reflections.

In addition, this study explored understandings of political bots through 15 interviews conducted during the politically sensitive period of the 2024 elections.⁶⁸¹ Future research could expand on this work by including a larger and more diverse group of participants to capture a broader range of perspectives. However, it may nevertheless be underlined that, in qualitative interview research, what is important is both the profile of the respondents and the relevance of their profiles to the research questions. This requirement was fulfilled in the present study. Furthermore, future research could provide insights into how perceptions of ethical principles, such as transparency, accountability, and trustworthy AI, change as legislation matures and public awareness of AI systems grows.

5.5. Concluding Comment

This study clearly shows that sustainable digital technologies require sufficient flexibility to adapt to ongoing and rapid technological advancements. However, flexibility alone is insufficient; it must be systematically integrated with other regulatory frameworks to form a coherent and responsive governance structure. Although this study did not aim to reach global conclusions, it provided recommendations specifically addressing legal gaps and potential practical vulnerabilities at both the EU and national levels within Europe.

The analysis revealed significant complexities in the AI Act's regulatory structure. Accordingly, the AI Act's comprehensive yet intricate framework has presented numerous

⁶⁸¹ Koh Ewe, 'The Ultimate Election Year: All the Elections Around the World in 2024' *Time* (28 December 2023) <<https://time.com/6550920/world-elections-2024/>>.

ambiguities regarding its applicability to political bots. These ambiguities should be addressed without further delay. Also, political bots, due to their multifunctional nature, pose unique categorisation challenges, often fitting simultaneously into multiple risk categories established by the AI Act. This complexity significantly hampers clarity in regulatory implementation. As a result, the research highlighted the necessity of clearer definitions and categorisations to enhance implementation effectiveness.

In addition, this research showed that democracy, beyond its existence as an ideal, has increasingly become a business area. Within this tendency, advertisements, computational propaganda, and other related methods form a multi-actor and multi-layered business model that includes legal gaps or grey areas legally. The research suggested a solution which is not to prohibit or eliminate this new version of democracy, but rather to place it within a framework that is compatible with democratic ideals and principles, even in digital age.

Thus, it seems protecting democracy in the digital era against political bots transcends single-domain considerations. It is necessary to approach comprehensively, recognising the essential intersections of law, technology, and democratic integrity. The AI Act represents a significant step toward addressing these intersections. However, the Act must be continually refined to consider emerging complexities and to protect democratic processes effectively from the evolving threats posed by political bots and AI-driven manipulation.

Bibliography

‘A Tech Accord to Combat Deceptive Use of AI in 2024 Elections - (Proposed for Public Signature and Announcement by Technology Companies at the Munich Security Conference on February 16, 2024)’

<<https://www.aielectionsaccord.com/#:~:text=This%20accord%20seeks%20to%20set,with%20their%20own%20policies%20and>>

Adeoye-Olatunde OA and Olenik NL, ‘Research and Scholarly Methods: Semi-structured Interviews’ (2021) 4 JACCP: Journal of the American College of Clinical Pharmacy 1358

<<https://doi.org/10.1002/jac5.1441>>

‘AI and the Audiovisual Sector: Navigating the Current Legal Landscape’ (IRIS 2024)

Akdeniz Y and Altıparmak K, *Internet: Restricted Access: A Critical Assessment of Internet Content Regulation and Censorship in Turkey* (IMAJ Yayinevi & IHOP 2008)

Alan Sears, ‘Algorithmic Speech and Freedom of Expression’ (2020) 53 Vanderbilt Law Review <<https://scholarship.law.vanderbilt.edu/vjtl/vol53/iss4/4>>

Alayna Treene, Kristen Holmes and Jeremy Herb, ‘How CEOs Are Trying to Be like Musk and Curry Favor with Trump’ *CNN* (21 December 2024)

<<https://edition.cnn.com/2024/12/21/politics/how-ceos-are-trying-to-be-like-musk-and-curry-favor-with-trump>>

‘Algorithmic Competition – Background Note’ (OECD Secretariat 2023)

<[https://one.oecd.org/document/DAF/COMP\(2023\)3/en/pdf](https://one.oecd.org/document/DAF/COMP(2023)3/en/pdf)>

Allcott H and Gentzkow M, ‘Social Media and Fake News in the 2016 Election’ (2017) 31 Journal of Economic Perspectives 211 <<https://doi.org/10.1257/jep.31.2.211>>

‘Analysis of Social Media Presence of Romanian Presidential Candidates’ *European Digital Media Observatory (EDMO)* (29 April 2025) <<https://edmo.eu/edmo-news/analysis-of-social-media-presence-of-romanian-presidential-candidates/>>

Andrea Vogt, ‘Hot or Bot? Italian Professor Casts Doubt on Politician’s Twitter Popularity’ *The Guardian* (Milan, 22 July 2012)

<<https://doi.org/https://www.theguardian.com/world/2012/jul/22/bot-italian-politician-twitter-grillo>>

Andreea Serban, Vasileios Rovilos and Katerina Demetzou, ‘Conformity Assessments under the EU AI Act: A Step-by Step Guide Updated with the Final Text of the AI Act’ (Future of Privacy Forum and OneTrust LLC 2025) White Paper <<https://fpf.org/wp-content/uploads/2025/04/OT-comformity-assessment-under-the-eu-ai-act-WP-1.pdf>>

Aneta Zachová, ‘TikTok Bots Push Anti-System Parties Ahead of Czech Elections’ *EURACTIV* (2 October 2025) <<https://www.euractiv.com/news/tiktok-bots-push-anti-system-parties-ahead-of-czech-elections/>>

Annette Kroeber-Riel, 'An Update on Political Advertising in the European Union' (14 November 2024) <<https://blog.google/around-the-globe/google-europe/political-advertising-in-eu/>>

'Approval of the Content of the Draft Communication from the Commission - Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)'

'Artificial Intelligence, Democracy and Elections' *European Parliament* (October 2023) <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI\(2023\)751478_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf)>

Assenmacher D and others, 'Demystifying Social Bots: On the Intelligence of Automated Social Media Actors' (2020) 6 *Social Media + Society* 205630512093926 <<https://doi.org/10.1177/2056305120939264>>

Bader S and Szabo L-V, 'Voter Manipulation and Electoral Campaign Hijacking by Social Media Technologies. The Romania 2024 Case' (2025) <<https://doi.org/10.2139/ssrn.5243802>> accessed 4 June 2025

Balkin JM, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' [2017] *SSRN Electronic Journal* <<https://doi.org/10.2139/ssrn.3038939>> accessed 20 September 2023

Banakar R, 'Having One's Cake and Eating It: The Paradox of Contextualisation in Socio-Legal Research' (2011) 7 *International Journal of Law in Context* 487 <<https://doi.org/10.1017/S1744552311000267>>

Barrett PM, Hendrix J and Richard- Carvajal C, 'Digital Risks to the 2024 Elections: Safeguarding Democracy in an Era of Disinformation' (NYU Center for Business and Human Rights 2024)

Başak Bozkurt, Diara J. Townes and Linda Li, 'Election Interference: How Tech, Race, and Disinformation Can Influence the U.S Election' (*Oxford Internet Institute*, October 2024) <<https://www.oii.ox.ac.uk/news-events/election-interference-how-tech-race-and-disinformation-can-influence-the-us-elections/>>

Bassini M, 'Speech without a Speaker: Constitutional Coverage for Generative AI Output?' [2025] *European Constitutional Law Review* 1 <<https://doi.org/10.1017/S1574019625100771>>

Bastos M and Mercea D, 'The Public Accountability of Social Platforms: Lessons from a Study on Bots and Trolls in the Brexit Campaign' (2018) 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 20180003 <<https://doi.org/10.1098/rsta.2018.0003>>

Bastos M, Mercea D and Baronchelli A, 'The Geographic Embedding of Online Echo Chambers: Evidence from the Brexit Campaign' (2018) 13 *PLOS ONE* e0206841 <<https://doi.org/10.1371/journal.pone.0206841>>

Bello BS and Heckel R, 'Analyzing the Behaviour of Twitter Bots in Post Brexit Politics' *2019 Sixth International Conference on Social Networks Analysis, Management and Security*

(SNAMS) (IEEE 2019) <<https://doi.org/10.1109/SNAMS.2019.8931874>> accessed 5 September 2023

Bennett CJ, 'Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America?' (2016) 6 International Data Privacy Law 261 <<https://doi.org/10.1093/idpl/ipw021>>

Bessi A and Ferrara E, 'Social Bots Distort the 2016 U.S. Presidential Election Online Discussion' [2016] First Monday <<https://doi.org/10.5210/fm.v21i11.7090>> accessed 1 September 2023

Bolsover G, 'Computational Propaganda in China: An Alternative Model of a Widespread Practice' (2017) Working Paper No. 2017.4

Bontridder N and Pouillet Y, 'The Role of Artificial Intelligence in Disinformation' (2021) 3 Data & Policy <<https://doi.org/10.1017/dap.2021.20>> accessed 21 July 2025

Bossetta M, Dutceac Segesten A and Trenz H-J, 'The Brexit Battle on Facebook: Assessing Echo Chambers and Polarisation' (19 June 2018) <<https://blogs.lse.ac.uk/brexit/2018/06/19/the-brexit-battle-on-facebook-assessing-echo-chambers-and-polarisation/>>

Bradshaw S and Howard PN, 'Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation' (Computational Propaganda Research Project of Oxford University)

Brandt SL, 'Donald Trump, the Reality Show: Populism as Performance and Spectacle' (2020) 50 Zeitschrift für Literaturwissenschaft und Linguistik 303 <<https://doi.org/10.1007/s41244-020-00170-3>>

Braun V and Clarke V, 'Using Thematic Analysis in Psychology' (2006) 3 Qualitative Research in Psychology 77 <<https://doi.org/10.1191/1478088706qp063oa>>

Brian O'Donovan, 'One-in-Five Voters Changed Ballot Choices Based on Social Media Posts - Survey' *RTE* (28 May 2024) <<https://www.rte.ie/news/ireland/2024/0522/1450493-election-social-media/>>

Brinkmann S and Kvale S, *Doing Interviews* (Uwe Flick ed, Second edition, SAGE 2018)

Brkan M, 'AI-Supported Decision-Making under the General Data Protection Regulation' *Proceedings of the 16th edition of the International Conference on Artificial Intelligence and Law* (ACM 2017) <<https://doi.org/10.1145/3086512.3086513>> accessed 19 October 2025

——, 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27 International Journal of Law and Information Technology 91 <<https://doi.org/10.1093/ijlit/eay017>>

Broniatowski DA and others, 'Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate' (2018) 108 American Journal of Public Health 1378 <<https://doi.org/10.2105/AJPH.2018.304567>>

Bruno M, Lambiotte R and Saracco F, 'Brexit and Bots: Characterizing the Behaviour of Automated Accounts on Twitter during the UK Election' (2022) 11 EPJ Data Science 17 <<https://doi.org/10.1140/epjds/s13688-022-00330-0>>

Bueno de Mesquita E, Canes-Wrone B and B. Hall A, 'Preparing for Generative AI in the 2024 Election' (Stanford Graduate School of Business and the University of Chicago Harris School of Public Policy November 2023) <https://harris.uchicago.edu/files/ai_and_elections_best_practices_no_embargo.pdf>

Buiten M, 'Combating Disinformation and Ensuring Diversity on Online Platforms: Goals and Limits of EU Platform' [2022] SSRN Electronic Journal <<https://doi.org/10.2139/ssrn.4009079>> accessed 1 March 2024

Cade Metz, 'OpenAI Starts Testing Ads in ChatGPT' *The New York Times* <<https://www.nytimes.com/2026/01/16/technology/chatgpt-ads-openai.html>>

Cammiss S and Watkins D, 'Legal Research In the Humanities' in Dawn Watkins (ed), *Research methods in law* (Routledge 2013)

Caprile A, 'Foreign Interference in EU Democratic Processes: Second Report' (European Parliament 2023) Plenary <[https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747908/EPRS_ATA\(2023\)747908_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747908/EPRS_ATA(2023)747908_EN.pdf)>

Carpentier CL, 'New Economics for Sustainable Development: Attention Economy' (the United Nations 2023) <https://www.un.org/sites/un2.un.org/files/attention_economy_feb.pdf>

Casiraghi MC, Curini L and Cusumano E, 'The Colors of Ideology: Chromatic Isomorphism and Political Party Logos' (2023) 29 Party Politics 463 <<https://doi.org/10.1177/13540688221080539>>

Catherine Kim, 'How Gen Z Became the Most Gullible Generation' (23 April 2025) <<https://www.politico.com/news/magazine/2025/04/23/gen-z-media-tiktok-misinformation-00287561>>

Celeste E, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2019) 33 International Review of Law, Computers & Technology 122 <<https://doi.org/10.1080/13600869.2018.1475898>>

—, *The Content Governance Dilemma: Digital Constitutionalism, Social Media and the Search for a Global Standard* (Springer Nature 2023)

Cerf V, 'PARRY Encounters the DOCTOR' (1973) Request for Comments: 439 NIC: 13771 <<https://www.rfc-editor.org/rfc/pdfrfc/rfc439.txt.pdf>>

Chen Z and Chen D, 'Identifying the Invisible: A Comprehensive Approach to Distinguishing Software Bots' (2024)

Chris Lunday, 'Putin's Bot Army Tries to Swing German Election' *POLITICO* (6 February 2025) <<https://www.politico.eu/article/germany-election-flood-social-media-x-russia-bots-kremlin-operation-false-news/>>

Chris Vallance, 'Face Search Company Clearview AI Overturns UK Privacy Fine' *BBC News* (18 October 2023) <<https://www.bbc.com/news/technology-67133157>>

Christiano T, 'Algorithms, Manipulation, and Democracy' (2022) 52 *Canadian Journal of Philosophy* 109 <<https://doi.org/10.1017/can.2021.29>>

Chu Z and others, 'Who Is Tweeting on Twitter: Human, Bot, or Cyborg?' *Proceedings of the 26th Annual Computer Security Applications Conference* (ACM 2010) <<https://doi.org/10.1145/1920261.1920265>> accessed 28 August 2023

——, 'Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?' (2012) 9 *IEEE Transactions on Dependable and Secure Computing* 811 <<https://doi.org/10.1109/TDSC.2012.75>>

'Code of Conduct for the 2024 European Parliament Elections' (International Institute for Democracy and Electoral Assistance (International IDEA) and the European Commission 2024) <https://commission.europa.eu/document/bebd9b72-fbb9-42f3-bcea-dbace7e0650f_en>

'Code of Practice for General-Purpose AI Models' (European Commission 2025) <<https://ec.europa.eu/newsroom/dac/redirection/document/118119>>

'Commission Guidelines on the Definition of an Artificial Intelligence System Established by Regulation (EU) 2024/1689 (AI Act)'

Costantino G, Martinelli F and Sgandurra D, 'Are Photos on Social Networks Really Private?' *2013 International Conference on Collaboration Technologies and Systems (CTS)* (IEEE 2013) <<https://doi.org/10.1109/CTS.2013.6567223>> accessed 6 May 2024

Council of the European Union, 'Council Conclusions on Safeguarding a Free and Pluralistic Media System' (2020) 13260/20 <<https://data.consilium.europa.eu/doc/document/ST-13260-2020-INIT/en/pdf>>

Cownie F and Bradney A, 'Socio-Legal Studies: A Challenge to the Doctrinal Approach' in Dawn Watkins (ed), *Research methods in law* (1st Edition, Routledge 2013)

Creswell JW, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed, SAGE Publications 2014)

Culloty E and Suiter J, *Disinformation and Manipulation in Digital Media: Information Pathologies* (Routledge 2021)

Cupać J and Sienknecht M, 'Regulate against the Machine: How the EU Mitigates AI Harm to Democracy' (2024) 31 *Democratization* 1067 <<https://doi.org/10.1080/13510347.2024.2353706>>

Curini L, Moffitt B and Zulianello M, 'The Colors of the Populist Radical Right: The Strategic Use of Hue and Saturation in Party Logos' (2025) 30 *The International Journal of Press/Politics* 819 <<https://doi.org/10.1177/19401612241229216>>

Dahlgren P, 'The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation' (2005) 22 *Political Communication* 147
<<https://doi.org/10.1080/10584600590933160>>

Dan Milmo, 'Elon Musk's AI Firm Blames Unauthorised Change for Chatbot's Rant about "White Genocide"' *The Guardian* (16 May 2025)
<<https://www.theguardian.com/technology/2025/may/16/elon-musks-ai-firm-blames-unauthorised-change-for-chatbots-rant-about-white-genocide>>

Dan Taylor, 'Op-Ed: The EU's Artificial Intelligence Act Does Little to Protect Democracy' *tech.eu* (14 March 2022) <<https://tech.eu/2022/03/14/op-ed-the-eu-s-artificial-intelligence-act-does-little-to-protect-democracy/>>

Darren O'Donovan and Darren O'Donovan, 'Socio-Legal Methodology: Conceptual Underpinnings, Justifications and Practical Pitfalls' in Laura Cahillane and Jennifer Schweppe (eds), *Legal research methods: principles and practicalities* (Clarus Press 2016)

'Data Brokers A Call for Transparency and Accountability' (Federal Trade Commission 2014) <<https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>>

'Data Protection Policy'

Davies P, 'The New EU AI Act Is under Threat from Lobbyists, Experts and the Public Agree' [2023] *Euronews* <<https://www.euronews.com/next/2023/11/29/europes-ai-act-under-threat-by-lobbyists-experts-and-the-public-say>>

——, 'The New EU AI Act Is under Threat from Lobbyists, Experts and the Public Agree' (3 December 2023) <<https://www.euronews.com/next/2023/11/29/europes-ai-act-under-threat-by-lobbyists-experts-and-the-public-say>>

Davis CA and others, 'BotOrNot: A System to Evaluate Social Bots'
<<https://doi.org/10.48550/ARXIV.1602.00975>> accessed 18 August 2023

De Vries K, 'Let the Robot Speak! AI-Generated Speech and Freedom of Expression' in Steffen Hindelang and Andreas Moberg (eds), *YSEC Yearbook of Socio-Economic Constitutions 2021*, vol 2021 (Springer International Publishing 2022)
<https://doi.org/10.1007/16495_2021_38> accessed 21 November 2023

Deryugina OV, 'Chatterbots' (2010) 37 *Scientific and Technical Information Processing* 143
<<https://doi.org/10.3103/S0147688210020097>>

Dickerson JP, Kagan V and Subrahmanian VS, 'Using Sentiment to Detect Bots on Twitter: Are Humans More Opinionated than Bots?' *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)* (IEEE 2014)
<<https://doi.org/10.1109/ASONAM.2014.6921650>> accessed 19 October 2025

Dicks B and others, *Qualitative Research and Hypermedia* (SAGE Publications, Ltd 2005)
<<https://doi.org/10.4135/9781849209649>> accessed 1 September 2025

Dietrich F, ‘AI-Based Removal of Hate Speech from Digital Social Networks: Chances and Risks for Freedom of Expression’ (2025) 5 AI and Ethics 2943
<<https://doi.org/10.1007/s43681-024-00610-7>>

‘Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines’ [2023] *European Commission-Press release*
<https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413>

Dijk J, ‘Tracing Twitter: The Rise of a Microblogging Platform’ (2011) 7 International Journal of Media & Cultural Politics 333 <https://doi.org/10.1386/macp.7.3.333_1>

Diurni A and Riccio G, ‘ChatGPT: Challenges and Legal Issues in Advanced Conversational AI’ (2023) 9 Italian Law Journal 473

Donlan SP and Heckendorn Urscheler L (eds), *Concepts of Law: Comparative, Jurisprudential, and Social Science Perspectives* (Routledge 2016)
<<https://doi.org/10.4324/9781315573298>>

Doshi J and others, ‘Sleeper Social Bots: A New Generation of AI Disinformation Bots Are Already a Political Threat’ (arXiv, 2024) <<https://doi.org/10.48550/ARXIV.2408.12603>>
accessed 2 March 2025

Dr Tugrulcan Elmas, *Grok Furkan Bölükbaşı’na Neden Küfretti? RAG ve Yapay Zekânın En Büyük Açığı (In English: Why Did Grok Swear at Furkan Bölükbaşı? What Are AI’s and RAG’s Biggest Security Vulnerability?)* (2025)
<https://www.youtube.com/watch?v=s65LH_Llf18#:~:text=Elon%20Musk%27%C4%B1n%20X%27e%20yerle%C5%9Ftirdi%C4%9Fi%20Yapay%20Zek%C3%A2%20edepsiz%20Grok%20Furkan%20B%C3%B6l%C3%BCkba%C5%9F%C4%B1%27na%20k%C3%BCfretti.%20Ama%20neden?>>

Draghi M, ‘The Future of European Competitiveness Part A | A Competitiveness Strategy for Europe’ (European Commission 2024)
<https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en>

‘DSA Elections Toolkit for Digital Services Coordinators Instruments, Best Practices, and Lessons Learnt’ (European Board on Digital Services 2025)

Dubois E and McKelvey F, ‘Political Bots: Disrupting Canada’s Democracy’ (2019) 44 Canadian Journal of Communication PP <<https://doi.org/10.22230/cjc.2019v44n2a3511>>

Dutkiewicz L and others, ‘Artificial Intelligence and Media’ in Nathalie A Smuha (ed), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (1st edn, Cambridge University Press 2025) <<https://doi.org/10.1017/9781009367783.018>> accessed 6 September 2025

Elklit J and Maley M, ‘Why Ballot Secrecy Still Matters’ (2019) 30 Journal of Democracy 61 <<https://doi.org/10.1353/jod.2019.0042>>

Elmas T, Overdorf R and Aberer K, ‘Characterizing Retweet Bots: The Case of Black Market Accounts’ (2022) 16 Proceedings of the International AAAI Conference on Web and Social Media 171 <<https://doi.org/10.1609/icwsm.v16i1.19282>>

Emilio Ferrara, 'How Twitter Bots Affected the US Presidential Campaign' *The Conversation* (8 November 2016) <<https://theconversation.com/how-twitter-bots-affected-the-us-presidential-campaign-68406>>

'Emotion Recognition Using Chatbot System', in Shraddha Pophale, Hetal Gandhi and Anil Kumar Gupta, *Advances in Intelligent Systems and Computing* (Springer Singapore 2021) <https://doi.org/10.1007/978-981-15-7234-0_54> accessed 26 July 2025

Erfort C, 'Targeting Voters Online: How Parties' Campaigns Differ' (2024) 92 Electoral Studies 102872 <<https://doi.org/10.1016/j.electstud.2024.102872>>

Erlenhov L, Neto FGDO and Leitner P, 'An Empirical Study of Bots in Software Development: Characteristics and Challenges from a Practitioner's Perspective' *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (ACM 2020) <<https://doi.org/10.1145/3368089.3409680>> accessed 1 May 2026

Ernst D and Sassen S (eds), 'The New Mobility of Knowledge: Digital Information Systems and Global Flagship Networks' *Digital Formations: IT and New Architectures in the Global Realm* (Princeton University Press 2005) <<https://doi.org/10.1515/9781400831616.89>> accessed 27 February 2025

'EU Action Plan on Human Rights and Democracy 2020-2024' <<https://www.consilium.europa.eu/media/46838/st12848-en20.pdf>>

European Commission, 'Commission Recommendation (EU) 2023/2829 of 12 December 2023 on Inclusive and Resilient Electoral Processes in the Union and Enhancing the European Nature and Efficient Conduct of the Elections to the European Parliament'

European Commission. Directorate General for Communications Networks, Content and Technology., 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust' (2020) COM(2020) 65 final

'European Convention on Human Rights'

European Court of Human Rights, 'Guide on Article 10 of the European Convention on Human Rights' (2022) <https://www.echr.coe.int/documents/guide_art_10_eng.pdf>

'European Democracy Action Plan' (European Commission 2020) <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790>>

European Parliament, Council of the European Union and European Commission, 'Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02)'

European Parliamentary Research Service, 'Children and Deepfakes' *European Parliament* (July 2025) <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI\(2025\)775855_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf)>

Ewe K, 'The Ultimate Election Year: All the Elections Around the World in 2024' *Time* (28 December 2023) <<https://time.com/6550920/world-elections-2024/>>

‘Exploring Twitter’s API for Academic Research Purposes’ (*X Developers*)
<<https://devcommunity.x.com/t/exploring-twitter-s-api-for-academic-research-purposes/224809>>

‘Facial Recognition: Italian SA Fines Clearview AI EUR 20 Million’ *European Data Protection Board* (10 March 2022) <https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en>

Farrand B, ‘Regulating Misleading Political Advertising on Online Platforms: An Example of Regulatory Mercantilism in Digital Policy’ (2024) 45 *Policy Studies* 730
<<https://doi.org/10.1080/01442872.2023.2258810>>

Federal Foreign Office, ‘Germany Targeted by the Pro-Russian Disinformation Campaign “Doppelgänger”’ (Federal Foreign Office 2024) Technical Report on an Analysis by the Federal Foreign Office <<https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf>>

Fernquist J and others, ‘Twitter Bots and the Swedish Election’ in Mohammad A Tayebi, Uwe Glässer and David B Skillicorn (eds), *Open Source Intelligence and Cyber Crime* (Springer International Publishing 2020) <https://doi.org/10.1007/978-3-030-41251-7_6> accessed 29 April 2026

Fernquist J, Kaati L and Schroeder R, ‘Political Bots and the Swedish General Election’ 2018 *IEEE International Conference on Intelligence and Security Informatics (ISI)* (IEEE 2018) <<https://doi.org/10.1109/ISI.2018.8587347>> accessed 20 April 2023

Ferrara E, ‘Disinformation and Social Bot Operations in the Run up to the 2017 French Presidential Election’ [2017] *First Monday* <<https://doi.org/10.5210/fm.v22i8.8005>> accessed 29 April 2026

——, ‘Should ChatGPT Be Biased? Challenges and Risks of Bias in Large Language Models’ (2023) 28 <<https://doi.org/https://doi.org/10.5210/fm.v28i11.13346>> accessed 13 December 2024

——, ‘Social Bot Detection in the Age of ChatGPT: Challenges and Opportunities’ [2023] *First Monday* <<https://doi.org/10.5210/fm.v28i6.13185>> accessed 26 November 2024

——, ‘The Rise of Social Bots’ (2016) 59 *Communications of the ACM* 96
<<https://doi.org/10.1145/2818717>>

Festinger L, ‘Cognitive Dissonance’ (1962) 207 *Scientific American* 93
<<https://doi.org/10.1038/scientificamerican1062-93>>

——, *A Theory of Cognitive Dissonance* (Reissued by Stanford Univ. Press in 1962, renewed 1985 by author, [Nachdr.], Stanford Univ Press 2001)

Firdaus VAH, Saputra PY and Suprianto D, ‘Intelligence Chatbot for Indonesian Law on Electronic Information and Transaction’ (2020) 830 *IOP Conference Series: Materials Science and Engineering* 022089 <<https://doi.org/10.1088/1757-899X/830/2/022089>>

Fleming-Jones J, 'EU AI Act Nearing Agreement despite Three Key Roadblocks – Co-Rapporteur' [2023] *Euronews* <<https://www.euronews.com/next/2023/10/23/eu-ai-act-nearing-agreement-despite-three-key-roadblocks-co-rapporteur>>

'Foreign Interference in All Democratic Processes in the European Union. European Parliament Resolution of 9 March 2022 on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation.'
<https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.pdf>

Forelle M and others, 'Political Bots and the Manipulation of Public Opinion in Venezuela' (arXiv, 2015) <<https://doi.org/10.48550/ARXIV.1507.07109>> accessed 16 June 2025

——, 'Political Bots and the Manipulation of Public Opinion in Venezuela' (arXiv, 2015) <<https://doi.org/10.48550/ARXIV.1507.07109>> accessed 19 October 2025

Foster R, 'Review: A New Structural Transformation of the Public Sphere and Deliberative Politics by Jürgen Habermas' (26 August 2024) <<https://oxfordpoliticalreview.com/2024/08/26/review-a-new-structural-transformation-of-the-public-sphere-and-deliberative-politics-by-jurgen-habermas/>>

Fowler A and Margolis M, 'The Political Consequences of Uninformed Voters' (2014) 34 *Electoral Studies* 100 <<https://doi.org/10.1016/j.electstud.2013.09.009>>

'Freedom of Expression and Information- Explanations' <<https://fra.europa.eu/en/eu-charter/article/11-freedom-expression-and-information#explanations>>

Gallagher A, *Web of Lies: The Lure and Danger of Conspiracy Theories* (GILL BOOKS 2022)

Galligan D, *Law in Modern Society* (Oxford University Press 2006) <<https://doi.org/10.1093/acprof:oso/9780199291830.001.0001>> accessed 19 November 2024

Gatt L and others, 'FRIA Implementation Model According to the AI Act' 2024 *IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRaine)* (IEEE 2024) <<https://doi.org/10.1109/MetroXRaine62247.2024.10796624>> accessed 24 September 2025

'General-Purpose Artificial Intelligence' (European Parliament March 2023) <[https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA\(2023\)745708_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf)>

Gillespie T, 'The Politics of "Platforms"' (2010) 12 *New Media & Society* 347 <<https://doi.org/10.1177/1461444809342738>>

——, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018)

Gizem Yardımcı and Altug Yalcintas, 'The Issue of Central Planning in Big Data Age (Büyük Veri Çağında Merkezi Planlama Meselesi: Dijital Korumacılık mı, Sansür mü?)' *Özne | Volume 33: Science and Society Studies*, vol 33 (Çizgi Kitabevi 2021)

Gizzi MC and Rädiker S (eds), *The Practice of Qualitative Data Analysis* (MAXQDA Press 2021) <<https://doi.org/10.36192/978-3-948768058>> accessed 4 March 2025

‘Global Government Affairs’ <<https://x.com/GlobalAffairs/status/1658208072215437314>>

Goldberg J, ‘Trump Turned Politics into Reality TV. Now Harris Is the Show to Watch’ *Los Angeles Times* (13 August 2024) <<https://www.latimes.com/opinion/story/2024-08-13/donald-trump-campaign-kamala-harris-polling>>

Gorwa R, ‘What Is Platform Governance?’ (2019) 22 *Information, Communication & Society* 854 <<https://doi.org/10.1080/1369118X.2019.1573914>>

Gotfredsen SG, ‘Harris Is Outspending Trump on Social Media. How Much Does That Matter?’ *Columbia Journalism Review* (24 October 2024) <https://www.cjr.org/the_media_today/harris_trump_social_media_ads_meta_google.php>

Graham T and Andrejevic M, ‘A Computational Analysis of Potential Algorithmic Bias on Platform X during the 2024 US Election [Working Paper] (Unpublished)’ (2024) <<https://eprints.qut.edu.au/253211/>>

Grigorie TL (ed), Zemčík, M.T. (2019). *A Brief History of Chatbots. International Conference on Artificial Intelligence, Control and Automation Engineering (AICAE 2019): June 23-24, 2019, Wuhan, China* (DEStech Publications, Inc 2019)

Grimme C and others, ‘Social Bots: Human-Like by Means of Human Control?’ (2017) 5 *Big Data* 279 <<https://doi.org/10.1089/big.2017.0044>>

Gulbrandsen IT and Just SN, ‘What Do We Know about Digital Public Debate? Technological Affordances and Democratic Dilemmas’ (2025) 46 *Nordicom Review* 148 <<https://doi.org/10.2478/nor-2025-0014>>

Habermas J, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (MIT Press 1989)

——, ‘Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere’ (2022) 39 *Theory, Culture & Society* 145 <<https://doi.org/10.1177/02632764221112341>>

Habermas J and Cronin C, *A New Structural Transformation of the Public Sphere and Deliberative Politics* (Polity Press 2024)

Hagen L and others, ‘Rise of the Machines? Examining the Influence of Social Bots on a Political Discussion Network’ (2022) 40 *Social Science Computer Review* 264 <<https://doi.org/10.1177/0894439320908190>>

Han Rongbin, ‘Manufacturing Consent in Cyberspace: China’s “Fifty-Cent Army”’ (2015) 44 *Journal of Current Chinese Affairs* 105 <<https://doi.org/10.1177/186810261504400205>>

Harris KR, ‘Liars and Trolls and Bots Online: The Problem of Fake Persons’ (2023) 36 *Philosophy & Technology* 35 <<https://doi.org/10.1007/s13347-023-00640-9>>

- Harth L and Kriener F, 'Responding to Foreign Interference in the EU: Beware of Unintended Consequences' *Carnegie Europe* (10 December 2022) <<https://carnegieeurope.eu/2022/10/12/responding-to-foreign-interference-in-eu-beware-of-unintended-consequences-pub-88101>>
- Hegelich S and Janetzko D, 'Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet' (2021) 10 *Proceedings of the International AAAI Conference on Web and Social Media* 579 <<https://doi.org/10.1609/icwsm.v10i1.14764>>
- Heidari M, Jones JHJ and Uzuner O, 'Online User Profiling to Detect Social Bots on Twitter' (arXiv, 2022) <<https://doi.org/10.48550/ARXIV.2203.05966>> accessed 2 March 2025
- Helberger N and Diakopoulos N, 'ChatGPT and the AI Act' (2023) 12 *Internet Policy Review* <<https://doi.org/10.14763/2023.1.1682>> accessed 31 March 2023
- Helberger N, Pierson J and Poell T, 'Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34 *The Information Society* 1 <<https://doi.org/10.1080/01972243.2017.1391913>>
- Helbing D, 'Globally Networked Risks and How to Respond' (2013) 497 *Nature* 51 <<https://doi.org/10.1038/nature12047>>
- 'High-Level Group on Media Freedom and Pluralism Terms of Reference' (High-Level Group on Media Freedom and Pluralism 2011) <https://ec.europa.eu/information_society/media_taskforce/doc/pluralism/hlg/hlg_tor.pdf>
- Himmelreich J, 'Against "Democratizing AI"' [2022] *AI & SOCIETY* <<https://doi.org/10.1007/s00146-021-01357-z>> accessed 14 November 2022
- 'How Different Age Groups Are Using Social Media 2024' *Target Internet* <<https://targetinternet.com/resources/how-different-age-groups-are-using-social-media-2024/>>
- Howard PN and others, 'Social Media, News and Political Information during the US Election: Was Polarizing Content Concentrated in Swing States?' <<https://doi.org/10.48550/ARXIV.1802.03573>> accessed 6 January 2023
- Howard PN and Kollanyi B, 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum' <<https://doi.org/10.48550/ARXIV.1606.06356>> accessed 1 September 2023
- Howard PN, Woolley S and Calo R, 'Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration' (2018) 15 *Journal of Information Technology & Politics* 81 <<https://doi.org/10.1080/19331681.2018.1448735>>
- , 'Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration' (2018) 15 *Journal of Information Technology & Politics* 81 <<https://doi.org/10.1080/19331681.2018.1448735>>

——, ‘Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration’ (2018) 15 *Journal of Information Technology & Politics* 81
<<https://doi.org/10.1080/19331681.2018.1448735>>

Hutchinson J, ‘Micro-Platformization for Digital Activism on Social Media’ (2021) 24 *Information, Communication & Society* 35
<<https://doi.org/10.1080/1369118X.2019.1629612>>

‘Inauthentic & Malign Influence Activity - Croatian Presidential Runoff’ (Center for Information Resilience 2024) <https://www.info-res.org/app/uploads/2025/01/Inauthentic_Behavior_-Croatian_Presidential_Runoff_v2.pdf>

‘Information Note on “Use of Generative Artificial Intelligence (AI) by Judicial Professionals in a Work- Related Context”’ (European Commission for the Efficiency of Justice(CEPEJ) Working group on Cyberjustice and Artificial Intelligence (CEPEJ-GT-CYBERJUST) 2024) CEPEJ-GT-CYBERJUST(2023)5final

Ingram D, ‘How Elon Musk Turned X into a Pro-Trump Echo Chamber’ *BNC News* (31 October 2024) <<https://www.nbcnews.com/tech/social-media/elon-musk-turned-x-trump-echo-chamber-rcna174321>>

‘INTERIM REPORT on the Proposal for a Council Decision Determining, Pursuant to Article 7(1) of the Treaty on European Union, the Existence of a Clear Risk of a Serious Breach by Hungary of the Values on Which the Union Is Founded’ (Committee on Civil Liberties, Justice and Home Affairs 2022) (C9-0000/2022 – 2018/0902R(NLE))
<https://web.archive.org/web/20230321060050/https://www.europarl.europa.eu/doceo/document/A-9-2022-0217_EN.html>

International Institute for Democracy and Electoral Assistance (International IDEA), ‘Code of Conduct for the 2024 European Parliament Elections’

Isabel Barberá, *AI Privacy Risks & Mitigations – Large Language Models (LLMs)* (European Data Protection Board 2025) <<https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf>>

Izadi S and Forouzanfar M, ‘Error Correction and Adaptation in Conversational AI: A Review of Techniques and Applications in Chatbots’ (2024) 5 *AI* 803
<<https://doi.org/10.3390/ai5020041>>

Jamieson KH and Cappella JN (eds), *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment* (Oxford University Press 2010)

Jean Tsang S, ‘Cognitive Discrepancy, Dissonance, and Selective Exposure’ (2019) 22 *Media Psychology* 394 <<https://doi.org/10.1080/15213269.2017.1282873>>

Jeff Howe, ‘The Rise of Crowdsourcing’ (1 June 2006)
<<https://www.wired.com/2006/06/crowds/>>

Jin S-AA and Phua J, ‘Following Celebrities’ Tweets About Brands: The Impact of Twitter-Based Electronic Word-of-Mouth on Consumers’ Source Credibility Perception, Buying

Intention, and Social Identification With Celebrities' (2014) 43 Journal of Advertising 181
<<https://doi.org/10.1080/00913367.2013.827606>>

Jones R, 'Why Do Qualitative Research?' (1995) 311 BMJ 2
<<https://doi.org/10.1136/bmj.311.6996.2>>

Jürgen Habermas, *Kamusalığın Yeni Bir Yapısal Dönüşümü ve Müzakereci Demokrasi* (1st Edition, İletişim Yayınları 2023)

Kaplan AM and Haenlein M, 'Users of the World, Unite! The Challenges and Opportunities of Social Media' (2010) 53 Business Horizons 59
<<https://doi.org/10.1016/j.bushor.2009.09.003>>

Karen Weise and Maggie Haberman, 'Amazon Plans \$1 Million Donation to Trump's Inaugural Fund' (12 December 2024)
<<https://www.nytimes.com/2024/12/12/technology/amazon-trump-inauguration.html>>

Karl Taro Greenfeld, 'The Network Effect' (10 April 2000)
<<https://time.com/archive/6740836/the-network-effect/>>

Kasap O and Yalcintas A, 'Commodification 2.0: How Does Spotify Provide Its Services for Free?' (2021) 53 Review of Radical Political Economics 157
<<https://doi.org/10.1177/0486613420924163>>

Katzenbach C and others, 'Policing Platforms: Addressing Power and Inequalities in Platform Policies' [2023] AoIR Selected Papers of Internet Research
<<https://doi.org/10.5210/spir.v2022i0.12959>> accessed 21 July 2025

Katzenbach C and Ulbricht L, 'Algorithmic Governance' (2019) 8 Internet Policy Review
<<https://doi.org/10.14763/2019.4.1424>> accessed 20 September 2023

Keller CI and Celeste E, 'Editorial | Editorial' (2019) 5 Revista Publicum ii
<<https://doi.org/10.12957/publicum.2019.47306>>

Keller TR and Klinger U, 'Social Bots in Election Campaigns: Theoretical, Empirical, and Methodological Implications' (2019) 36 Political Communication 171
<<https://doi.org/10.1080/10584609.2018.1526238>>

Kenny R and others, 'Duped by Bots: Why Some Are Better than Others at Detecting Fake Social Media Personas' (2024) 66 Human Factors: The Journal of the Human Factors and Ergonomics Society 88 <<https://doi.org/10.1177/00187208211072642>>

Kenrick Cai, 'Meta Introduces Llama Application Programming Interface to Attract AI Developers' *Reuters* (29 April 2025) <<https://www.reuters.com/business/meta-introduces-llama-application-programming-interface-attract-ai-developers-2025-04-29/>>

Kerr A, De Paoli S and Keatinge M, 'Surveillant Assemblages of Governance in Massively Multiplayer Online Games: A Comparative Analysis' (2014) 12 Surveillance & Society 320
<<https://doi.org/10.24908/ss.v12i3.4953>>

Kircher R, 'Questionnaires to Elicit Quantitative Data' in Lena Zipp and Ruth Kircher (eds), *Research Methods in Language Attitudes* (1st edn, Cambridge University Press 2022) <<https://doi.org/10.1017/9781108867788>> accessed 6 March 2025

Kirk N, 'Lobbying and the Online Influence Industry – Reactionary Regulation of Data Driven Political Campaigns' (*publicpolicy.ie*, 10 January 2023) <<https://publicpolicy.ie/governance/lobbying-and-the-online-influence-industry-reactionary-regulation-of-data-driven-political-campaigns/>>

Klykken FH, 'Implementing Continuous Consent in Qualitative Research' (2022) 22 *Qualitative Research* 795 <<https://doi.org/10.1177/14687941211014366>>

Kollanyi B, Howard PN and Woolley SC, 'Bots and Automation over Twitter during the Third U.S. Presidential Debate' [2016] COMPROP DATA MEMO 2016.3 / 27 OCT 2016 <<https://demtech.oii.ox.ac.uk/research/posts/bots-and-automation-over-twitter-during-the-third-u-s-presidential-debate/>>

Kollanyi B, N. Howard P and Woolley SC, 'Bots and Automation over Twitter during the U.S. Election' (2016) 2016.4 <<https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2016/11/Data-Memo-US-Election.pdf>>

Koltay A, 'Freedom of Speech: The Unreachable Mirage' [2013] SSRN Electronic Journal <<https://doi.org/10.2139/ssrn.2216655>> accessed 8 December 2022

Kosinski M, 'Facial Recognition Technology Can Expose Political Orientation from Naturalistic Facial Images' (2021) 11 *Scientific Reports* 100 <<https://doi.org/10.1038/s41598-020-79310-1>>

Kreiss D, 'Micro-Targeting, the Quantified Persuasion' (2017) 6 *Internet Policy Review* <<https://doi.org/10.14763/2017.4.774>> accessed 13 February 2024

Kris Shrishak, 'EU's AI Act: Tread the Guidelines Lightly' *Tech Policy Press* (21 February 2025) <<https://www.techpolicy.press/eu-ai-act-tread-the-guidelines-lightly/>>

Kuckartz U and Rädiker S, *Analyzing Qualitative Data with MAXQDA: Text, Audio, and Video* (Springer 2019)

Kusal S and others, 'A Systematic Review of Applications of Natural Language Processing and Future Challenges with Special Emphasis in Text-Based Emotion Detection' (2023) 56 *Artificial Intelligence Review* 15129 <<https://doi.org/10.1007/s10462-023-10509-0>>

Kwon D, 'Web-Scraping AI Bots Cause Disruption for Scientific Databases and Journals' (2025) 642 *Nature* 281 <<https://doi.org/10.1038/d41586-025-01661-4>>

Lamo M and Calo R, 'Regulating Bot Speech' (2019) 66 *UCLA Law Review* 988

Langbroek P and others, 'Editorial Methodology of Legal Research: Challenges and Opportunities' (2017) 13 *Utrecht Law Review* 1 <<https://doi.org/10.18352/ulr.411>>

Lauer M, Renda A and Yeung T, 'Clarifying the Costs for the EU's AI Act' [2021] *Centre for European Policy Studies (CEPS)* <<https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/>>

- Lebeuf C, Storey M-A and Zagalsky A, 'Software Bots' (2018) 35 IEEE Software 18
<<https://doi.org/10.1109/MS.2017.4541027>>
- Lebeuf CR, 'A Taxonomy of Software Bots: Towards a Deeper Understanding of Software Bot Characteristics' (Master of Science, University of Victoria 2013)
<https://chisel.cs.uvic.ca/theses/Lebeuf_Carlene_MSc_2018.pdf>
- LeCompte MD, 'Analyzing Qualitative Data' (2000) 39 Theory Into Practice 146
<https://doi.org/10.1207/s15430421tip3903_5>
- Lee K, Eoff B and Caverlee J, 'Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter' (2011) 5 Proceedings of the International AAAI Conference on Web and Social Media 185 <<https://doi.org/10.1609/icwsm.v5i1.14106>>
- Leingang R, 'X's AI Chatbot Spread Voter Misinformation – and Election Officials Fought Back' (12 September 2024) <<https://www.theguardian.com/us-news/2024/sep/12/twitter-ai-bot-grok-election-misinformation>>
- Lessig L, 'Rendering Sensible Salient' (2018) 27 The Good Society 171
<<https://doi.org/10.5325/goodsociety.27.1-2.0171>>
- Lessio N and Morris A, 'Toward Design Archetypes for Conversational Agent Personality' 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (IEEE 2020)
<<https://doi.org/10.1109/SMC42975.2020.9283254>> accessed 31 August 2023
- Levy A and Kolodny L, 'Elon Musk Is \$70 Billion Richer since Trump Victory Due to Tesla Stock Surge' CNBC (11 November 2024) <<https://www.cnbc.com/2024/11/11/elon-musk-is-70-billion-richer-since-trump-victory-due-to-tesla-surge.html>>
- Lewins A and Silver C, *Using Software in Qualitative Research: A Step-by-Step Guide* (2. ed, SAGE 2014)
- Linus Wahlberg, 'Twitter Bots as a Threat to Democracy: How Political Bots on Twitter Jeopardized Democratic Functions of the Online Public Sphere during the 2022 Swedish General Election' (Master's Thesis, Uppsala University 2022)
- Lisa-Maria N. Neudert, 'Computational Propaganda in Germany: A Cautionary Tale' (2017) Computational Propaganda Research Project Working Paper No. 2017.7
- Lisa-Maria Neudert, Bence Kollanyi and Philip N. Howard, 'Junk News and Bots during the German Parliamentary Election: What Are German Voters Sharing over Twitter?' (University of Oxford 2017)
- Liu J and others, 'Conceptualizing Echo Chambers and Information Cocoons: A Literature Review and Synthesis of Current Knowledge and Future Directions' (2025) 34 The Journal of Strategic Information Systems 101904 <<https://doi.org/10.1016/j.jsis.2025.101904>>
- Long K and others, "'Could You Define That in Bot Terms?': Requesting, Creating and Using Bots on Reddit' *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (ACM 2017) <<https://doi.org/10.1145/3025453.3025830>> accessed 16 July 2025

- Lucy Y, 'Demonstrating Validity in Qualitative Psychology' in Jonathan A Smith (ed), *Qualitative Psychology: A Practical Guide to Research Methods* (SAGE Publications 2008)
- Mainz JT, Sønnderholm J and Uhrenfeldt R, 'Artificial Intelligence and the Secret Ballot' (2024) 39 *AI & SOCIETY* 515 <<https://doi.org/10.1007/s00146-022-01551-7>>
- Mancosu M and Vegetti F, 'What You Can Scrape and What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data' (2020) 6 *Social Media + Society* 2056305120940703 <<https://doi.org/10.1177/2056305120940703>>
- Mansell R and others, 'Information Ecosystems and Troubled Democracy A Global Synthesis of the State of Knowledge on News Media, AI and Data Governance' (The International Observatory on Information and Democracy, 2024)
- Mantelero A, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 *Computer Law & Security Review* 106020 <<https://doi.org/10.1016/j.clsr.2024.106020>>
- Maria Martinez, 'Germany's Far-Right AfD Rises to Record 28%, INSA Poll Shows' *Reuters* (25 April 2026) <<https://www.reuters.com/world/germanys-far-right-afd-rises-record-28-insa-poll-shows-2026-04-25/>>
- Mariano-Florentino Cuéllar and Aziz Z. Huq, 'The Democratic Regulation of Artificial Intelligence' (*Knight First Amendment Institute at Columbia University*, 31 January 2022) <<https://knightcolumbia.org/content/the-democratic-regulation-of-artificial-intelligence>>
- Mariëtte van Huijstee and others, 'Tackling Deepfakes in European Policy' (European Parliamentary Research Service 2021) <[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU\(2021\)690039_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf)>
- Mather L, 'Law and Society' in Robert Goodin (ed), *The Oxford Handbook of Political Science* (1st edn, Oxford University Press 2013) <<https://doi.org/10.1093/oxfordhb/9780199604456.013.0015>> accessed 20 October 2025
- Mauldin ML, 'ChatterBots, TinyMuds, and the Turing Test: Entering the Loebner Prize Competition.' (1994)
- Maunz S, "'It Has To Have A Soul": How Chatbots Get Their Personalities' *npr* (10 March 2017) <<https://www.npr.org/sections/alltechconsidered/2017/03/10/519002884/it-has-to-have-a-soul-how-chatbots-get-their-personalities>>
- Maxwell JA, 'Designing a Qualitative Study.' 2 *The SAGE handbook of applied social research methods* 214
- 'Maynooth University Research Ethics Policy (Version: 2)'
- McAleese S and Kilty J, 'Stories Matter: Reaffirming the Value of Qualitative Research' [2019] *The Qualitative Report* <<https://doi.org/10.46743/2160-3715/2019.3713>> accessed 6 October 2025

McConville M and Chui WH (eds), *Research Methods for Law* (Third edition, Edinburgh University Press 2024) <<https://doi.org/10.1515/9781399515092>>

Merriam SB and Tisdell EJ, *Qualitative Research: A Guide to Design and Implementation* (Fourth edition, John Wiley & Sons 2016)

META, Newsroom for Europe, Middle East and Africa, 'Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation' (25 July 2025) <<https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>>

Michael Lipka and Kristen Eddy, 'Relatively Few Americans Are Getting News from AI Chatbots like ChatGPT' (*Pew Research Centre*, 1 October 2025) <https://www.pewresearch.org/short-reads/2025/10/01/relatively-few-americans-are-getting-news-from-ai-chatbots-like-chatgpt/?utm_source=Pew+Research+Center&utm_campaign=e278e753fc-EMAIL_CAMPAIGN_2025_10_02_06_52&utm_medium=email&utm_term=0_3e953b9b70-e278e753fc-400659657>

Miller T and Boulton M, 'Changing Constructions of Informed Consent: Qualitative Research and Complex Social Worlds' (2007) 65 *Social Science & Medicine* 2199 <<https://doi.org/10.1016/j.socscimed.2007.08.009>>

Mitchell M, 'Analyzing the Law Qualitatively' (2023) 23 *Qualitative Research Journal* 102 <<https://doi.org/10.1108/QRJ-04-2022-0061>>

Monaco N and Woolley SC, *Bots* (Polity Press 2022)

Moore M, '8. Protecting Democratic Legitimacy in a Digital Age' (2019) 90 *The Political Quarterly* 92 <<https://doi.org/10.1111/1467-923X.12572>>

Moore M and Tambini D, *Regulating Big Tech: Policy Responses to Digital Dominance* (First edition, Oxford University Press 2022)

Morgan H, 'Conducting a Qualitative Document Analysis' [2022] *The Qualitative Report* <<https://doi.org/10.46743/2160-3715/2022.5044>> accessed 6 March 2025

Muldoon J, Graham M and Cant C, *Feeding the Machine: The Hidden Human Labour Powering AI* (Canongate 2024)

Na SH, Cho S and Shin S, 'Evolving Bots: The New Generation of Comment Bots and Their Underlying Scam Campaigns in YouTube' *Proceedings of the 2023 ACM on Internet Measurement Conference* (ACM 2023) <<https://doi.org/10.1145/3618257.3624822>> accessed 24 April 2026

Narayan J and Larsen B, 'Generative AI: A Game-Changer That Society and Industry Need to Be Ready For' (*World Economic Forum*, 9 January 2023) <<https://www.weforum.org/stories/2023/01/davos23-generative-ai-a-game-changer-industries-and-society-code-developers/>>

Natale S, 'If Software Is Narrative: Joseph Weizenbaum, Artificial Intelligence and the Biographies of ELIZA' (2019) 21 *New Media & Society* 712 <<https://doi.org/10.1177/1461444818804980>>

Navon S and Noy C, 'Conceptualizing Social Media Sub-Platforms: The Case of Mourning and Memorialization Practices on Facebook' (2023) 25 *New Media & Society* 2898 <<https://doi.org/10.1177/14614448211035769>>

Nenadić I, 'Unpacking the "European Approach" to Tackling Challenges of Disinformation and Political Manipulation' (2019) 8 *Internet Policy Review* <<https://doi.org/10.14763/2019.4.1436>> accessed 19 October 2025

'New Allegations of Russian Interference in the European Parliament, in the Upcoming EU Elections and the Impact on the European Union (2024/2696(RSP))' (European Parliament 2024) <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0380_EN.html>

Ngo T and others, 'Spot the Bot: Investigating User's Detection Cues for Social Bots and Their Willingness to Verify Twitter Profiles' (2023) 146 *Computers in Human Behavior* 107819 <<https://doi.org/10.1016/j.chb.2023.107819>>

Nicole S and Liebe U, 'Going Digital: Web Data Collection Using Twitter as an Example' (2020) <<http://policy-practice.oxfam.org.uk/publications/going-digital-web-data-collection-using-twitter-as-an-example-620948>>

'No Ifs, Many Bots? Partisan Bot-like Accounts Continue to Amplify Divisive Content on X, Generating over 4 Billion Views since the UK General Election Was Called' (Global Witness 2024) <<https://www.globalwitness.org/en/campaigns/digital-threats/no-ifs-many-bots-partisan-bot-accounts-continue-amplify-divisive-content-x-generating-over-4-billion-views-uk-general-election-was-called/>>

Oliver DG, Serovich JM and Mason TL, 'Constraints and Opportunities with Interview Transcription: Towards Reflection in Qualitative Research' (2005) 84 *Social Forces* 1273 <<https://doi.org/10.1353/sof.2006.0023>>

'Opinion of Advocate General Saugmandsgaard Øe Republic of Poland v. European Parliament, Council of the European Union'

Orabi M and others, 'Detection of Bots in Social Media: A Systematic Review' (2020) 57 *Information Processing & Management* 102250 <<https://doi.org/10.1016/j.ipm.2020.102250>>

Paolo Cesarini, 'Propaganda and Disinformation: Lessons from 2024/25 Elections in Europe' *European Digital Media Observatory (EDMO)* (10 June 2025) <<https://edmo.eu/edmo-news/propaganda-and-disinformation-lessons-from-2024-25-elections-in-europe/>>

Papakyriakopoulos O, 'Political Machines: A Framework for Studying Politics in Social Machines' (2022) 37 *AI & SOCIETY* 113 <<https://doi.org/10.1007/s00146-021-01180-6>>

Pastor-Galindo J and others, 'Spotting Political Social Bots in Twitter: A Use Case of the 2019 Spanish General Election' (2020) 17 *IEEE Transactions on Network and Service Management* 2156 <<https://doi.org/10.1109/TNSM.2020.3031573>>

Paul M. Barrett and others, ‘Digital Risks to the 2024 Elections: Safeguarding Democracy in an Era of Disinformation’ (NYU Center for Business and Human Rights 2024) <<https://bhr.stern.nyu.edu/publication/digital-risks-to-the-2024-elections-safeguarding-democracy-in-the-era-of-disinformation/>>

Peers S and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2021) <<https://doi.org/10.5040/9781509933495>> accessed 10 November 2022

Pelin Ünker and Thomas Sparrow and May 24, 2023, ‘Fact Check: Turkey’s Erdogan Shows False Kilicdaroglu Video’ *Deutsche Welle* <<https://www.dw.com/en/fact-check-turkeys-erdogan-shows-false-kilicdaroglu-video/a-65554034>>

Persily N, ‘Can Democracy Survive the Internet?’ (2017) 28 *Journal of Democracy* 63 <<https://doi.org/10.1353/jod.2017.0025>>

Persily N and Tucker JA (eds), ‘Bots and Computational Propaganda: Automation for Communication and Control’ *Social Media and Democracy: The State of the Field, Prospects for Reform* (1st edn, Cambridge University Press 2020) <<https://doi.org/10.1017/9781108890960>> accessed 27 August 2023

—— (eds), *Social Media and Democracy: The State of the Field, Prospects for Reform* (1st edn, Cambridge University Press 2020) <<https://doi.org/10.1017/9781108890960>> accessed 26 April 2023

Pescetelli N, Barkoczi D and Cebrian M, ‘Bots Influence Opinion Dynamics without Direct Human-Bot Interaction: The Mediating Role of Recommender Systems’ (2022) 7 *Applied Network Science* 46 <<https://doi.org/10.1007/s41109-022-00488-6>>

Philip Selznick, ‘“Law in Context” Revisited’ (2003) 30 *Journal of Law and Society* 177

Philipp Hacker, Atoosa Kasirzadeh and Lilian Edwards, ‘AI, Digital Platforms, and the New Systemic Risk (Last Revised: 23 Sep 2025)’ <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5475049>

Pierson J and others, ‘Governing Artificial Intelligence in the Media and Communications Sector’ (2023) 12 *Internet Policy Review* <<https://doi.org/10.14763/2023.1.1683>> accessed 21 March 2023

Pierson J, Kerr A and Heyman R, ‘Meeting Societal Expectations: Cooperative Responsibility in the Design and Governance of AI’ (2020) <<https://researchportal.vub.be/en/publications/meeting-societal-expectations-cooperative-responsibility-in-the-d>>

Pineda A, Hermida A and Bellido-Pérez E, ‘Visualizing Political Communication on Spanish Social Media: An Analysis of Andalusian Political Parties’ *Communication on Instagram* [2025] *Visual Communication* 14703572241307305 <<https://doi.org/10.1177/14703572241307305>>

Platform X Global Government Affairs, ‘Global Government Affairs’ (23 March 2025) <<https://x.com/GlobalAffairs/status/1903879657755230507?s=20>>

POLITICO Staff, 'Incoming National Security Adviser's Son Spreads Fake News about D.C. Pizza Shop' *POLITICO* (12 April 2016) <<https://www.politico.com/story/2016/12/incoming-national-security-advisers-son-spreads-fake-news-about-dc-pizza-shop-232181>>

Pope C, 'Qualitative Research in Health Care: Analysing Qualitative Data' (2000) 320 *BMJ* 114 <<https://doi.org/10.1136/bmj.320.7227.114>>

Pouget H and Zuhdi R, 'AI and Product Safety Standards Under the EU AI Act' *Carnegie Europe* <<https://carnegieendowment.org/2024/03/05/ai-and-product-safety-standards-under-eu-ai-act-pub-91870>>

Prior M, *Post-Broadcast Democracy: How Media Choice Increases Inequality in Political Involvement and Polarizes Elections* (Reprint, Cambridge University Press 2008)

Prummer A, 'Micro-Targeting and Polarization' (2020) 188 *Journal of Public Economics* 104210 <<https://doi.org/10.1016/j.jpubeco.2020.104210>>

Rakhra M and others, 'E-Commerce Assistance with a Smart Chatbot Using Artificial Intelligence' 2021 *2nd International Conference on Intelligent Engineering and Management (ICIEM)* (IEEE 2021) <<https://doi.org/10.1109/ICIEM51511.2021.9445316>> accessed 1 May 2026

Rapley T, *Doing Conversation, Discourse and Document Analysis* (2nd edition, SAGE 2018)

Rapley TJ, 'The Art(Fulness) of Open-Ended Interviewing: Some Considerations on Analysing Interviews' (2001) 1 *Qualitative Research* 303 <<https://doi.org/10.1177/146879410100100303>>

Ratkiewicz J and others, 'Truthy: Mapping the Spread of Astroturf in Microblog Streams' *Proceedings of the 20th international conference companion on World wide web* (ACM 2011) <<https://doi.org/10.1145/1963192.1963301>> accessed 31 August 2023

Rauchfleisch A and Kaiser J, 'The False Positive Problem of Automatic Bot Detection in Social Science Research' (2020) 15 *PLOS ONE* e0241045 <<https://doi.org/10.1371/journal.pone.0241045>>

'Recommendation No. R (2000) 7 of the Committee of Ministers to Member States on the Right of Journalists Not to Disclose Their Sources of Information' (Council of Europe 2000) <<https://rm.coe.int/16805e2fd2>>

'Regulating Disinformation with Artificial Intelligence' (European Parliament 2019) STUDY Panel for the Future of Science and Technology European Science-Media Hub <[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU\(2019\)624279_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf)>

Reisach U, 'The Responsibility of Social Media in Times of Societal and Political Manipulation' (2021) 291 *European Journal of Operational Research* 906 <<https://doi.org/10.1016/j.ejor.2020.09.020>>

'Report of the Work Undertaken by the ChatGPT Taskforce' (European Data Protection Board 2024)

‘Research and Commercialisation Conflict of Interest: Policy and Guidelines (Revised:2019)’

Research Committee, ‘Maynooth University Research Integrity Policy’

Risse M, ‘Artificial Intelligence and the Past, Present, and Future of Democracy’ in Silja Voenekey and others (eds), *The Cambridge Handbook of Responsible Artificial Intelligence* (1st edn, Cambridge University Press 2022) <<https://doi.org/10.1017/9781009207898.009>> accessed 20 October 2025

Risso L, ‘Harvesting Your Soul? Cambridge Analytica and Brexit’ *Brexit Means Brexit?* (Akademie der Wissenschaften und der Literatur 2018)

Risto Uuk, ‘Manipulation and the AI Act’ (The Future of Life Institute 2022)

Robert Booth, ‘Experts Warn of Threat to Democracy from “AI Bot Swarms” Infesting Social Media’ *The Guardian* (22 January 2026) <<https://www.theguardian.com/technology/2026/jan/22/experts-warn-of-threat-to-democracy-by-ai-bot-swarms-infesting-social-media>>

Robert Brennan and Rabhya Mehrotra, ‘What Media Sources Did People Use & Trust before Voting in 2024 General Election?’ *RTE* (5 June 2025) <<https://www.rte.ie/brainstorm/2025/0605/1516628-national-election-and-democracy-study-media-use-trust-general-election-2024/>>

Roberts J, ‘The Erosion of Ethics: From Citizen Journalism to Social Media’ (2019) 17 *Journal of Information, Communication and Ethics in Society* 409 <<https://doi.org/10.1108/JICES-01-2019-0014>>

Robins-Early N and Leingang R, ‘Elon Musk Is Trump’s Biggest Cheerleader. How Could He Affect Election Results?’ *The Guardian* (18 October 2024) <<https://www.theguardian.com/us-news/ng-interactive/2024/oct/18/elon-musk-trump-election-influence>>

Robinson P, Seib P and Frohlich R (eds), ‘Social Media, Revolution, and the Rise of the Political Bot’ *Routledge Handbook of Media, Conflict and Security* (0 edn, Routledge 2016) <<https://doi.org/10.4324/9781315850979>> accessed 31 August 2023

Rodríguez-Ruiz J and others, ‘A One-Class Classification Approach for Bot Detection on Twitter’ (2020) 91 *Computers & Security* 101715 <<https://doi.org/10.1016/j.cose.2020.101715>>

Ross Arguedas A and others, ‘Echo Chambers, Filter Bubbles, and Polarisation: A Literature Review’ (Reuters Institute for the Study of Journalism 2022) <<https://doi.org/10.60625/RISJ-ETXJ-7K60>> accessed 7 May 2026

Ross B and others, ‘Are Social Bots a Real Threat? An Agent-Based Model of the Spiral of Silence to Analyse the Impact of Manipulative Actors in Social Networks’ (2019) 28 *European Journal of Information Systems* 394 <<https://doi.org/10.1080/0960085X.2018.1560920>>

Rossi S and others, 'Detecting Political Bots on Twitter during the 2019 Finnish Parliamentary Election' (2020) <<https://doi.org/10.24251/HICSS.2020.298>> accessed 19 October 2025

Rowbottom J, 'Government Speech and Public Opinion: Democracy by the Bootstraps' (2017) 25 *Journal of Political Philosophy* 22 <<https://doi.org/10.1111/jopp.12101>>

Saeed M and others, 'Crowdsourced Fact-Checking at Twitter: How Does the Crowd Compare With Experts?' *Proceedings of the 31st ACM International Conference on Information & Knowledge Management* (ACM 2022) <<https://doi.org/10.1145/3511808.3557279>> accessed 7 May 2026

Salmi J, 'A Democratic Way of Controlling Artificial General Intelligence' (2023) 38 *AI & SOCIETY* 1785 <<https://doi.org/10.1007/s00146-022-01426-x>>

Samantha Bradshaw and Philip N. Howard, 'The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation' (Oxford Internet Institute 2019) Computational Propaganda Research Project

Samuel Woolley and Dean Jackson, 'We Research AI Election Threats. Here's What We Need to Prepare for' *The Guardian* (9 October 2025) <<https://www.theguardian.com/commentisfree/2025/oct/09/artificial-intelligence-research-election-threats>>

Sanovich S, 'Computational Propaganda in Russia: The Origins of Digital Misinformation' Working Paper Working Paper No. 2017.3

Sayeh Yousefi, Ben Tappin and Jens Madsen, 'How AI Is Shaping Elections' (*LSE Blogs*, 8 May 2026) <<https://blogs.lse.ac.uk/politicsandpolicy/how-ai-is-shaping-elections/>>

Schäfer F, Evert S and Heinrich P, 'Japan's 2014 General Election: Political Bots, Right-Wing Internet Activism, and Prime Minister Shinzō Abe's Hidden Nationalist Agenda' (2017) 5 *Big Data* 294 <<https://doi.org/10.1089/big.2017.0049>>

Schaich Borg J, Sinnott-Armstrong W and Conitzer V, *Moral AI: And How We Get There* (Pelican, an imprint of Penguin Books 2024)

Schellekens MHM, 'Are Internet Robots Adequately Regulated?' (2013) 29 *Computer Law & Security Review* 666 <<https://doi.org/10.1016/j.clsr.2013.09.003>>

Seden Akcinaroglu and others, 'An Exploration of the Influence of Misinformation and Detering Technologies' (2023) <https://www.cmu.edu/ideas-social-cybersecurity/events/ideas2023_paper_8501.pdf>

Seers K, 'Qualitative Data Analysis' (2012) 15 *Evidence Based Nursing* 2 <<https://doi.org/10.1136/ebnurs.2011.100352>>

Select Committee on Intelligence United States Senate, 'Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election Volume:2 Russia's Use of Social Media with Additional View' (2020) 116–XX <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf>

Shao C and others, 'The Spread of Low-Credibility Content by Social Bots' (2018) 9 Nature Communications 4787 <<https://doi.org/10.1038/s41467-018-06930-7>>

Shattock E, 'The Electoral Commission, Disinformation and Freedom of Expression' (2021) 71 Northern Ireland Legal Quarterly 675 <<https://doi.org/10.53386/nllq.v71i4.543>>

——, 'Should the ECtHR Invoke Article 17 for Disinformation Cases?' (*EJIL Talk: Blog of European Journal of International Law*, 26 March 2021) <https://www.ejiltalk.org/should-the-ecthr-invoke-article-17-for-disinformation-cases/?utm_source=mailpoet&utm_medium=email&utm_campaign=ejil-talk-newsletter-post-title_2>

Shiroma Silva, 'Trump's Twitter Debate Lead Was "Swelled by Bots"' *BBC News* (18 October 2016) <<https://www.bbc.com/news/technology-37684418>>

Silvija Vuković, 'Celebrity Populism and Leadership: Analyzing the Interplay of Celebrity Politics and Populism in Contemporary Political Communication' (PhD Thesis, Charles University 2025) <<http://hdl.handle.net/20.500.11956/201166>>

Simon FM, "'We Power Democracy": Exploring the Promises of the Political Data Analytics Industry' (2019) 35 The Information Society 158 <<https://doi.org/10.1080/01972243.2019.1582570>>

Skovfoged MM and others, 'Supporting Understanding: Comparing Conversational Interviewing in Chatbot vs Human-Administered Patient-Reported Outcomes for Stroke Survivors' [2026] *ACM Transactions on Computing for Healthcare* 3799983 <<https://doi.org/10.1145/3799983>>

Sophie James, 'Big Tech Emerges from US Election as New Powerbroker' *centralnews* <<https://centralnews.com.au/2024/11/14/big-tech-emerges-from-us-election-as-new-powerbroker/>>

Stacy Hein, 'A Qualitative Study on How Micro-Influencers Detect Bots on LinkedIn' (PhD Thesis, Department of Doctoral Studies, Colorado Technical University 2023) <<https://may.idm.oclc.org/login?url=https://www.proquest.com/dissertations-theses/qualitative-study-on-how-micro-influencers-detect/docview/2864746549/se-2?accountid=12309>>

Stella M, Ferrara E and De Domenico M, 'Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems' (2018) 115 *Proceedings of the National Academy of Sciences* 12435 <<https://doi.org/10.1073/pnas.1803470115>>

——, 'Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems' (2018) 115 *Proceedings of the National Academy of Sciences* 12435 <<https://doi.org/10.1073/pnas.1803470115>>

Stier S and others, 'Election Campaigning on Social Media: Politicians, Audiences, and the Mediation of Political Communication on Facebook and Twitter' (2018) 35 *Political Communication* 50 <<https://doi.org/10.1080/10584609.2017.1334728>>

Stukal D and others, 'The Use of Twitter Bots in Russian Political Communication Online' (PONARS Eurasia Policy Memo 2019) 564

- , ‘For Whom the Bot Tolls: A Neural Networks Approach to Measuring Political Orientation of Twitter Bots in Russia’ (2019) 9 SAGE Open 215824401982771 <<https://doi.org/10.1177/2158244019827715>>
- , ‘Why Botter: How Pro-Government Bots Fight Opposition in Russia’ (2022) 116 American Political Science Review 843 <<https://doi.org/10.1017/S0003055421001507>>
- Subrahmanian VS and others, ‘The DARPA Twitter Bot Challenge’ <<https://doi.org/10.48550/ARXIV.1601.05140>> accessed 19 October 2025
- Sudmann A (ed), *The Democratization of Artificial Intelligence: Net Politics in the Era of Learning Algorithms*, vol 1 (1st edn, transcript Verlag 2019) <<https://doi.org/10.14361/9783839447192>> accessed 20 October 2025
- Tarja Laaninen, ‘Media Literacy Fostering a Key Civic Skill in a Digital Information Environment’ (European Parliament 2025) Briefing PE 772.886 <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772886/EPRS_BRI\(2025\)772886_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772886/EPRS_BRI(2025)772886_EN.pdf)>
- Tatel DS, ‘The Right to Vote’ (2015) 159 Proceedings of the American Philosophical Society
- Taylor R, ‘The Brexit Battle on Facebook: Assessing Echo Chambers and Polarisation’ (*LSE BREXIT Blog*, 19 June 2018) <<https://blogs.lse.ac.uk/brexit/2018/06/19/the-brexit-battle-on-facebook-assessing-echo-chambers-and-polarisation/>>
- Thales Company, ‘Bad Bot Report’ (imperva 2020) <<https://www.imperva.com/resources/resource-library/reports/2020-bad-bot-report/>>
- , ‘Bad Bot Report’ (imperva 2024) <<https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/>>
- The Council of Europe, ‘The Framework Convention on Artificial Intelligence’ (*The Council of Europe*) <<https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>>
- ‘The French SA Fines Clearview AI EUR 20 Million’ *European Data Protection Board* (October 2022) <https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en>
- ‘The General-Purpose AI Code of Practice’ *EU Commission* (9 September 2025) <<https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai#ecl-inpage-the-3-chapters-of-the-code>>
- ‘The Grand National Assembly of Turkey Minutes Magazine (Türkiye Büyük Millet Meclisi Tutanak Dergisi)’
- ‘The Guardian View on Turkey’s Election: An End to Erdoğan’s Authoritarianism?’ *The Guardian* (11 May 2023) <<https://www.theguardian.com/commentisfree/2023/may/11/the-guardian-view-on-turkeys-election-an-end-to-erdogans-authoritarianism>>
- ‘The Oversight Board’ (<https://www.oversightboard.com/>)

- ‘The Status of Journalists in Europe’ (Council of Europe 2018) Doc. 14505
<<https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24287&lang=en>>
- ‘The Strengthened Code of Practice on Disinformation 2022’ (European Commission 2022)
<<https://ec.europa.eu/newsroom/dae/redirection/document/87585>>
- Tim Wu, ‘Machine Speech’ (2013) 161 University of Pennsylvania Law Review
<https://scholarship.law.upenn.edu/penn_law_review/vol161/iss6/2>
- Toffler A, *The Third Wave* (W Morrow 1980)
- Torbjörn Sjöström, ‘The Rise of Populism – A Presentation by Torbjörn Sjöström, from Novus and Gallup Nordic.’ (WAPOR 78th Annual Conference, St. Louis, Missouri, USA, 12 May 2025) <<https://youtu.be/bzjNIIPZGzk?si=nHtKZ5WN6HKF0YGX>>
- Tsirtsis S and others, ‘AI-Mediated Communication Can Steer Collective Opinion’ (arXiv, 2026) <<https://doi.org/10.48550/ARXIV.2605.16245>> accessed 19 July 2026
- Tucker J and others, ‘Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature’ [2018] SSRN Electronic Journal
<<https://doi.org/10.2139/ssrn.3144139>> accessed 15 September 2023
- Tufekci Z, ‘Engineering the Public: Big Data, Surveillance and Computational Politics’ [2014] First Monday <<https://doi.org/10.5210/fm.v19i7.4901>> accessed 7 December 2022
- Turing AM, ‘Computing Machinery and Intelligence’ (1950) 59 Mind 433
- ‘User Profile Images and Banners’ (*X Developer Platform*)
<<https://developer.twitter.com/en/docs/twitter-api/v1/accounts-and-users/user-profile-images-and-banners>>
- Van J, ‘Platform Mechanisms’ in José Van Dijck, Thomas Poell and Martijn De Waal, *The Platform Society* (1st edn, Oxford University Press New York 2018)
<<https://doi.org/10.1093/oso/9780190889760.003.0003>> accessed 20 October 2025
- Van Vooren L, ‘(Dis)Information Warfare Why Online Disinformation Is Able to Prosper and How to Fight It’ (University of Bologna 2022)
- Varol O, ‘Should We Agree to Disagree about Twitter’s Bot Problem?’ (2023) 37–38 Online Social Networks and Media 100263 <<https://doi.org/10.1016/j.osnem.2023.100263>>
- Vukčević I, ‘Facebook Oversight Board’s Decision on the Indefinite Suspension of Donald Trump’s Account’ (2021) 12 Pravni zapisi 295 <<https://doi.org/10.5937/pravzap0-32521>>
- Vuković S, ‘Celebrities Turning into Populists: The Celebrity Populism of Miroslav Škoro during the 2019 Croatian Presidential Campaign’ (2022) 13 Medijske studije 50
<<https://doi.org/10.20901/ms.13.25.3>>
- Wagner C and others, ‘When Social Bots Attack: Modeling Susceptibility of Users in Online Social Networks’ (2012)

Walker S, 'A Constructivist Grounded Theory of the Influences and Practices That Are Thought to Promote a Sense of Belonging in a Primary School Context' (University of Essex 2019)

Wallace RS, 'The Anatomy of A.L.I.C.E..' *Parsing the Turing Test* (2007)
<https://doi.org/10.1007/978-1-4020-6710-5_13>

Wardle C and AbdAllah A, 'The Information Environment and Its Influence on Misinformation Effects' in Tina D Purnat, Tim Nguyen and Sylvie Briand (eds), *Managing Infodemics in the 21st Century* (Springer International Publishing 2023)
<https://doi.org/10.1007/978-3-031-27789-4_4> accessed 7 September 2025

Watson A, 'Most Used Platforms to Access News in the Last Week in EU Member States as of October 2023, by Age Group' <<https://www.statista.com/statistics/1399401/news-platform-access-eu-by-age/>>

Wessel M and others, 'The Power of Bots: Characterizing and Understanding Bots in OSS Projects' (2018) 2 Proceedings of the ACM on Human-Computer Interaction 1
<<https://doi.org/10.1145/3274451>>

Westwood SJ, 'The Potential Existential Threat of Large Language Models to Online Survey Research' (2025) 122 Proceedings of the National Academy of Sciences e2518075122
<<https://doi.org/10.1073/pnas.2518075122>>

'What Happened on TikTok around the Annulled Romanian Presidential Election? An Investigation and Poll' *Global Witness* (17 December 2024)
<<https://globalwitness.org/en/campaigns/digital-threats/what-happened-on-tiktok-around-the-annulled-romanian-presidential-election-an-investigation-and-poll/>>

Willig C, *Introducing Qualitative Research in Psychology: Adventures in Theory and Method* (Second ed, Open university press 2008)

Woolley S, *Manufacturing Consensus: Understanding Propaganda in the Era of Automation and Anonymity* (Yale University Press 2023)

Woolley SC, 'Automating Power: Social Bot Interference in Global Politics' [2016] First Monday <<https://doi.org/10.5210/fm.v21i4.6161>> accessed 25 February 2025

Woolley SC and Howard PN (eds), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (Oxford University Press 2019)

——, 'Computational Propaganda Worldwide: Executive Summary' Working Paper 2017.11

'X DSA Researcher Application' (xAI) <https://docs.google.com/forms/d/e/1FAIpQLSdo0O-D6Kxa3cV4g1JLz2T_0Sk3hdEnTdv8dJmibagCnzJ7kg/viewform>

Yang M, 'Which Celebrities Have Endorsed Kamala Harris and Donald Trump? Here Are the Biggest Names' *The Guardian* (3 November 2024) <<https://www.theguardian.com/us-news/2024/nov/03/celebrity-endorsements-harris-trump>>

Yang X, Yang Q and Wilson C, ‘Penny for Your Thoughts: Searching for the 50 Cent Party on Sina Weibo’ (2021) 9 Proceedings of the International AAAI Conference on Web and Social Media 694 <<https://doi.org/10.1609/icwsm.v9i1.14649>>

Yannakakis GN and Togelius J, *Artificial Intelligence and Games* (Springer International Publishing 2018) <<https://doi.org/10.1007/978-3-319-63519-4>> accessed 1 May 2026

Yarchi M, Wolfsfeld G and Samuel-Azran T, ‘Not All Undecided Voters Are Alike: Evidence from an Israeli Election’ (2021) 38 Government Information Quarterly 101598 <<https://doi.org/10.1016/j.giq.2021.101598>>

Yardımcı G, ‘Avrupa İnsan Hakları Mahkemesi kararlarıyla serbest seçim hakkı (in English “The right to free elections in the decisions of the European Court of Human Rights”)’ (Unpublished master’s thesis, Ankara University 2020)

Yardımcı G, Kerr A and Mangan D, ‘The Social Science Deficit in AI Regulation: An Analysis of the Composition of the European Commission’s High-Level Group of Experts on Artificial Intelligence and Implications for Technology Regulation.’ (2023 conferences of the International Association for Media and Communication Research (IAMCR), Lyon, 9 July 2023) <<https://iamcr.org/node/30133>>

Yardımcı-Geyikçi Ş and Yavuziyılmaz H, ‘The 2023 Turkish Election: A Tale of Two Campaigns and the Duel of Populisms’ (2024) 24 Southeast European and Black Sea Studies 259 <<https://doi.org/10.1080/14683857.2024.2315650>>

Yardley L, ‘Demonstrating the Validity of Qualitative Research’ (2017) 12 The Journal of Positive Psychology 295 <<https://doi.org/10.1080/17439760.2016.1262624>>

Yener AÖ, Najafi A and Varol O, ‘City-Level User Location Detection from Social Media and Analysis of Political Participation’ 2024 32nd Signal Processing and Communications Applications Conference (SIU) (IEEE 2024) <<https://doi.org/10.1109/SIU61531.2024.10600825>> accessed 8 September 2025

Yılmaz Z and Turner BS, ‘Turkey’s Deepening Authoritarianism and the Fall of Electoral Democracy’ (2019) 46 British Journal of Middle Eastern Studies 691 <<https://doi.org/10.1080/13530194.2019.1642662>>

You J, Lee K and Kwon H-Y, ‘DeepScraper: A Complete and Efficient Tweet Scraping Method Using Authenticated Multiprocessing’ (2024) 149 Data & Knowledge Engineering 102260 <<https://doi.org/10.1016/j.datak.2023.102260>>

Yuliia Dukachc, ‘How TikTok Is Turning into an AI Dump. A Study of a Russian-Language Pirate TikTok Farm’ (*Teksmu.org.ua*, 10 May 2024) <<https://texty.org.ua/articles/112437/how-tiktok-turning-ai-dump-study-russian-language-pirate-tiktok-farm/>>

Zaller JR, *The Nature and Origins of Mass Opinion* (1st edn, Cambridge University Press 1992) <<https://doi.org/10.1017/CBO9780511818691>> accessed 21 July 2026

Zarei K, Farahbakhsh R and Crespi N, ‘How Impersonators Exploit Instagram to Generate Fake Engagement?’ *ICC 2020 - 2020 IEEE International Conference on Communications*

(ICC) (IEEE 2020) <<https://doi.org/10.1109/ICC40277.2020.9149431>> accessed 24 April 2026

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (First edition, PublicAffairs 2019)

——, ‘Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization’ (2022) 3 *Organization Theory* 26317877221129290 <<https://doi.org/10.1177/26317877221129290>>

Artificial Intelligence Act 2024 [2024/1689]

Charter of Fundamental Rights of the European Union [2012/C 326/02] (Document C2012/326/02)

Committee on Artificial Intelligence (CAI), Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law 2024 [CM(2024)52-final]

Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts 2023

Corrigendum to the position of the European Parliament Artificial Intelligence Act 2024 (cor01)

European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) {SWD(2025) 836 final} 2025 [COM(2025) 836 final] (2025/0359 (COD))

Neighbourhood, Development and International Cooperation Instrument (NDICI) 2021 [2021/947]

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 (2016/679)

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) 2022 [2000/31/EC]

Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising 2024 [Document 32024R0900]

Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021 (COM/2021/206 Final)

Handyside v United Kingdom Application No 5493/72 (European Court of Human Rights)

Sunday Times v the United Kingdom (No 1) , Application No 6538/74 (European Court of Human Rights)

The Sunday Times v The United Kingdom, Application no 6538/74 (European Court of Human Rights)

Federal Republic of Germany v European Parliament and Council of the European Union [2000] Court of Justice of the European Union (CJEU) Case C-376/98

Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland [2008] Court of Justice of the European Union (CJEU) C-73/07

Herri Batasuna and Batasuna v Spain Application No 25803/04 and 25817/04 (European Court of Human Rights)

Manole and Others v Moldova, Application No 13936/02 (European Court of Human Rights)

Al-Saadoon and Mufdhi v the United Kingdom, Application No 61498/08 (European Court of Human Rights)

Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) v Land Hessen
References for a preliminary ruling: Verwaltungsgericht Wiesbaden - Germany [2010] Court of Justice of the European Union (CJEU) 2010 I-11063

Björk Eiðsdóttir v Iceland Application No 46443/09 (European Court of Human Rights)

Case No VI ZR 269/12 (German Federal Court of Justice)

Delvigne v Commune de Lesparre Médoc and Préfet de la Gironde [2015] Court of Justice of the European Union (CJEU) C-650/13

Yavaş v Turkey Application No 16576/15 (European Court of Human Rights)

Magyar Bizottság v Hungary, Application No 18030/11 (European Court of Human Rights)

Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland, Application no 931/13
(The European Court of Human Rights)

Peter Nowak v Data Protection Commissioner [2017] Court of Justice of the European Union (CJEU) C-434/16

Demirtaş v Turkey, Application No 14305/17 (European Court of Human Rights)

Sergejs Buivids v Datu valsts inspekcija [2019] Court of Justice of the European Union (CJEU) Case C-345/17

Eva Glawischnig-Piesczek v Facebook Ireland Limited (Court of Justice of the European Union (CJEU))

Balaskas v Greece, Application No 73087/17 (European Court of Human Rights)

Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) [2020] Court of Justice of the European Union (CJEU) C-61/19

Former President Trump's suspension [2021] The Oversight Board case 2021-001-FB-FBR

Melike v Turkey Application No 35786/19 (European Court of Human Rights)

Gonzalez v Google LLC [2023] Supreme Court of the United States 21-1333

Twitter, Inc v Taamneh [2023] Supreme Court of the United States 21-1496

Appendices

Annex I - Interview Information Sheet



Annex I

Annex I

Interview Information Sheet

Researcher: Gizem YARDIMCI, PhD student, Maynooth University, Ireland.

Dear Participant,

Thank you for taking the time to consider participating in an interview as part of my PhD project. My project is “Regulating the influence of bots around political elections in the European Union”.

I am a PhD researcher in the Department of Law and Criminology, at Maynooth University in Ireland. I am undertaking a PhD under the supervision of Dr David MANGAN and Professor Aphra KERR. This research is interdisciplinary with supervision from both the School of Law and Criminology and the Department of Sociology. This PhD is funded by Science Foundation Ireland, a public research agency in Ireland. I am funded through the Centre for Research Training in Advanced Networks for Sustainable Societies (ADVANCE CRT).

The study focuses on the utilization of software robots, commonly referred to as 'bots', in political elections, particularly examining their prevalence in the European Union (EU). Bots can be easily created and controlled, often forming bot armies, for rapid and extensive social media engagement. However, there are concerns that bots can be used to influence political discussions and to manipulate voters decision-making processes. According to previous research, they could pose a threat to the integrity of political elections, although identifying the actors behind these bots is often challenging.

Accordingly, this research focuses on how political bots are being used as a tool to influence or manipulate political elections in the EU and what technical, legal or other interventions have been, or should be, developed to mitigate their harmful impacts. Additionally, this research explores if regulation can provide an effective instrument to prevent political bots from being used as a tool for manipulation without interfering with information pluralism and freedom of speech and information.

The main goals of the research are to present a detailed socio-legal analysis of the potential influence of EU’s regulations on political bots from the perspective of freedom of speech and information, to gather insights into online and automated threats to free elections and to provide recommendations to policy makers on how to protect the integrity of voting and elections in European democracies.

What will your participation in the study involve?

The interview is expected to last approximately one hour. It will be conducted online (via Microsoft Teams) or in-person (whichever is most convenient), and, if consent is given, it will be audio-recorded using a digital recording device and transcribed. All interviewees will be asked basic demographic questions and general questions regarding the research topic. Then, other questions will be tailored to you depending on your expertise or experience. Interviewees will be provided with a copy of their interview transcript afterwards upon request.

Who has approved this study?

This study has received ethical approval from Maynooth University Research Ethics Committee.

Why have you been asked to take part?

You have been asked to take part for this study because your expertise in, and experience with AI, will be beneficial to this research. In particular, I am interested in your views about the potential influence of the EU's regulations on political bots from the perspective of freedom of speech and information and your assessment about the potential influence of bots on elections.

Do you have to take part?

No, you are under no obligation whatsoever to take part in this research. You are invited to participate in a one-to-one interview with a researcher. It is entirely up to you to decide whether or not you would like to take part. If you decide to do so, you will be asked to sign a consent form and will be given a copy of the information sheet for your own records. If you decide to take part, you are still free to withdraw at any time without giving a reason and/or to withdraw your information up until such time as the research is submitted for examination, which should be by the 31st October 2025. This research study does not provide any form of remuneration or compensation to participants for their involvement.

What information will be collected?

Data will be gathered using face to face semi-structured interviews and online (via Microsoft Teams) interviews.

Your interview will be audio-recorded using a digital recording device and transcribed if consent is given for this. The gathered data will be anonymised to ensure that participants cannot be identified. This will assure you of the confidentiality of your participation. With the required precautions, no transcripts or identifiable details will be available to any person outside of the researcher and their supervisors. The recording will be stored securely by the researcher using Maynooth University's secure IT infrastructures, and in accordance with European and national data protection regulations and guidelines.

Measures will be taken to protect the recording and any personal information contained within it from unauthorized access or disclosure in accordance with Maynooth University Data

Procedures and Maynooth University Data Protection Policy. All primary data (anonymised where relevant and feasible) will be held for a minimum period of ten years following

publication. To secure data, passwords, and backup, appropriate anti-virus software in place will be used. Data collected on a mobile device will be encrypted, and the data will be protected with a strong password. Then, data will be removed from the mobile device and transferred to a secure IT server infrastructure at Maynooth University for storage.

Any identifiable references to people, places, events etc will be anonymised with pseudonyms.

Will your participation in the study be kept confidential?

Yes, all information that is collected about you during the course of the research will be kept confidential. No information will be distributed to any other unauthorised individual or third party. If you so wish, the data that you provide can also be made available to you at your own discretion.

'It must be recognised that, in some circumstances, confidentiality of research data and records may be overridden by courts in the event of litigation or in the course of investigation by lawful authority. In such circumstances the University will take all reasonable steps within the law to ensure that confidentiality is maintained to the greatest possible extent.'

What will happen to the information which you give?

All the information you provide will be kept securely, using password protection and encryption at Maynooth University. It will not be possible to identify you. On completion of the research, the anonymized data will be retained on a secure MU server for a period of 10 years.

After ten years, all data will be destroyed (by my supervisors). Manual data will be shredded confidentially, and electronic data will be reformatted or overwritten by my supervisors in Maynooth University.

If consent is given, the anonymised data you provide may also be deposited in the Irish Qualitative Data Archive (iqda@mu.ie). Maynooth University Social Sciences Institute (MUSSI) is a founding member of the archive. When data is deposited in an archive other researchers can read the transcripts and can use them in their own research projects. They may also be used by lecturers in their teaching.

What will happen to the results?

The research will be written up as my PhD thesis, and some of the findings will be presented at national and international conferences and may be published in scientific journals. A copy of the research findings as ongoing or completed publications will be made available to you upon request.

What are the possible disadvantages of taking part?

I do not envisage any negative consequences for you in taking part.

What if there is a problem?

At the end of the interview, I will discuss with you how you found the experience and how you are feeling. If you experience any distress following the interview, I can provide some information on appropriate supports.

If you feel the research has not been carried out as described above you may wish to contact my supervisors Dr David MANGAN (david.mangan@mu.ie) and/or PROFESSOR Aphra KERR (aphra.kerr@mu.ie).

Any further queries?

If you need any further information, you can contact me: Gizem YARDIMCI, gizem.yardimci.2022@mumail.ie.

If you agree to take part in the study, please complete and sign the consent form overleaf.

Thank you for taking the time to read this.

Consent Form [*Amend appropriately for your study*]

I.....agree to participate in Gizem YARDIMCI's research study titled Regulating manipulative political bots around political elections: The Artificial Intelligence Act and the EU Charter.

Please tick each statement below :

The purpose and nature of the study has been explained to me verbally & in writing. I've been able to ask questions, which were answered satisfactorily.

☐

I am participating voluntarily.

☐

I give permission for my interview with Gizem YARDIMCI to be audio recorded.

☐

I understand that I can withdraw from the study, without repercussions, at any time, whether that is before it starts or while I am participating.

☐

I understand that I can withdraw permission to use the data right up to research completion on 31 October 2025.

☐

It has been explained to me how my data will be managed and that I may access them on request.

☐

I understand the limits of confidentiality as described in the information sheet.

☐

I agree to quotation/publication of extracts from my interview.

☐

OR

I do not agree to quotation/publication of extracts from my interview.

☐

I understand that my data, in an anonymous format, may be used in further research projects and any subsequent publications if I give permission below.

☐

[*Select as appropriate*]

I agree for my data to be used for further research projects.

☐

OR

I do not agree for my data to be used for further research projects.

☐

I agree for my data, once anonymized, to be retained indefinitely in the Irish Qualitative Data Archive (IQDA) ☐

OR

I do not agree for my data once anonymised, to be retained indefinitely in the IQDA archive.

☐

Signed.....

Date.....

Participant Name in block capitals

I the undersigned have taken the time to fully explain to the above participant the nature and purpose of this study in a manner that they could understand. I have explained the risks involved as well as the possible benefits. I have invited them to ask questions on any aspect of the study that concerned them.

Signed.....

Date.....

Researcher Name in block capitals

If during your participation in this study you feel the information and guidelines that you were given have been neglected or disregarded in any way, or if you are unhappy about the process, please contact the Secretary of the Maynooth University Ethics Committee at research.ethics@mu.ie or +353 (0)1 708 6019. Please be assured that your concerns will be dealt with in a sensitive manner.

For your information the Data Controller for this research project is Maynooth University, Maynooth, Co. Kildare. The Data Protection office is located in Room 27, Rye Building, North Campus, Maynooth University, which can be contacted at dataprotection@mu.ie. Maynooth University Data Privacy policies can be found at <https://www.maynoothuniversity.ie/data-protection>.

Annex II - Ethical Approval

MAYNOOTH UNIVERSITY RESEARCH ETHICS COMMITTEE

MAYNOOTH UNIVERSITY,
MAYNOOTH, CO. KILDARE, IRELAND



Dr Carol Barrett
Secretary to Maynooth University Research Ethics Committee

14 June 2023

Gizem Yardimci
School of Law and Criminology
Maynooth University

Re: Application for ethical approval for a Project entitled: Regulating manipulative political bots around political elections: The Artificial Intelligence (AI) Act and the EU Charter

Dear Gizem,

The above project has been evaluated under Tier 2 process, expedited review and we would like to inform you that ethical approval has been granted.

Any deviations from the project details submitted to the ethics committee will require further evaluation. This ethical approval will expire on 30/09/2025.

Please note: all projects now require an end of project report which is attached. Please complete and upload the end of project report to your RIS ethics record after the project end date.

Kind Regards,

A handwritten signature in purple ink, appearing to read "Carol Barrett".

Dr Carol Barrett
Secretary,
Maynooth University Research Ethics Committee

c.c. Dr Aphra Kerr, Department of Sociology
Dr David Mangan, Department of Sociology

Reference Number SRESC-2023-36516

Annex III - Interview Questions for SG1

Interview questions are prepared for the three distinct sub-groups, including

1. National Policymakers, Advisers, Rapporteurs, or Former or Current Members of the Relevant Working Groups or Relevant Institutions Across the European Union,
2. Representatives of Non-Governmental Organisations (NGOs),
3. Representatives or Staff of Companies developing AI tools

The questions in section 1 and section 2 will be directed to all interviewees. Some sub-sections are designed for specific interviewees.

The questions in sub-section 1 will be addressed to national policymakers, advisers, rapporteurs, or former or current members of the relevant working groups or relevant institutions across the European Union. The questions in sub-section 2 will be addressed to representatives of Non-Governmental Organisations (NGOs). The questions in sub-section 3 will be addressed to representatives or staff of companies developing AI tools.

COMMON SECTIONS

Common Section-1: Questions for all interviewees:

1. What is your current job title and responsibilities?
2. How long have you been working in your current job?
3. Was your previous employment experience related to technology or AI?
4. What qualifications, training or degree do you have that are relevant to your current position?
5. Are you following Artificial Intelligence (AI) technological development closely because of your job or any personal interest in AI?
6. How would you define AI?
7. Are you watching or informed on regulatory developments about AI or other new technologies?
8. Do you believe it is possible to regulate AI?
9. What do you know about bots?

Common Section-2: Questions for all interviewees:

1. What impact can AI have on the development of bots?
2. Have you ever interacted with a bot before?
3. What is your knowledge about the use of bots?
4. What do you think about the using of bots on various digital platforms such as Telegram, Slack, Twitter, and Facebook?
5. If a bot is used for political purposes, what would you think of it?
6. What is your opinion on the use of political bots in elections?
7. How do you think the use of political bots can affect the public opinion?
8. Do you think the use of bots for political campaigns or to communicate online during elections should be regulated? If yes, how should this be done?
9. Do you think that the legal documents or policies of the EU provide any protection against the use of political bots in elections?

Sub- Section 1- Questions for National Policymakers, Advisers, Rapporteurs or Former or Current Members of the Relevant Working Groups or Relevant Institutions Across the European Union

1. Does your country have any regulations about bots? If yes, do you find it effective?
2. Does your country have any entities, initiatives or policies and principles to control the use of political bots in elections?
3. What steps has your government, or any other institution, taken to prevent the potential negative impacts of political bots on elections in general?
4. Does your government provide elections that are transparent and accountable to the public?
5. Does your government protect fundamental rights against using political bots?
6. Is the concept of "media blackout" applicable or relevant in the context of social media?
7. Does your government or institution attempt to protect voters' rights against potential online manipulations during political elections?
8. To what extent do you believe the draft AI Act can meet your expectations and will it be effective?
9. Can we consider political bots as AI systems which are used for democratic processes in Annex III of the draft AI Act?
10. How do you classify political bots in terms of the risk categories in the draft AI Act?

Annex IV - Interview Questions for SG2

Interview questions are prepared for the three distinct sub-groups, including

1. National Policymakers, Advisers, Rapporteurs, or Former or Current Members of the Relevant Working Groups or Relevant Institutions Across the European Union,
2. Representatives of Non-Governmental Organisations (NGOs),
3. Representatives or Staff of Companies developing AI tools

The questions in section 1 and section 2 will be directed to all interviewees. Some sub-sections are designed for specific interviewees.

The questions in sub-section 1 will be addressed to national policymakers, advisers, rapporteurs, or former or current members of the relevant working groups or relevant institutions across the European Union. The questions in sub-section 2 will be addressed to representatives of Non-Governmental Organisations (NGOs). The questions in sub-section 3 will be addressed to representatives or staff of companies developing AI tools.

COMMON SECTIONS

Common Section-1: Questions for all interviewees:

1. What is your current job title and responsibilities?
2. How long have you been working in your current job?
3. Was your previous employment experience related to technology or AI?
4. What qualifications, training or degree do you have that are relevant to your current position?
5. Are you following Artificial Intelligence (AI) technological development closely because of your job or any personal interest in AI?
6. How would you define AI? Mass knowledge of data very high level.
7. Are you watching or informed on regulatory developments about AI or other new technologies?
8. Do you believe it is possible to regulate AI?
9. What do you know about bots?

Common Section-2: Questions for all interviewees:

1. What impact can AI have on the development of bots?
2. Have you ever interacted with a bot before?
3. What is your knowledge about the use of bots?
4. What do you think about the using of bots on various digital platforms such as Telegram, Slack, Twitter, and Facebook?
5. If a bot is used for political purposes, what would you think of it?
6. What is your opinion on the use of political bots in elections?
7. How do you think the use of political bots can affect the public opinion?
8. Do you think the use of bots for political campaigns or to communicate online during elections should be regulated? If yes, how should this be done?
9. Do you think that the legal documents or policies of the EU provide any protection against the use of political bots in elections? Politic parties

Sub- Section 2- Questions for Representatives of NGOs:

1. Do you think the election processes in your country are democratic and fair for candidates and voters?
2. Do you think automated and intelligence online tools can affect the election results or election processes?
3. In your professional opinion, how do NGOs approach the potential impact of AI technology on democratic processes?
4. What can NGOs do about the political parties' strategies for using political bots in elections?
5. Do you have any consultation with official public authorities on the effects of political bots?
6. Do you have any concerns in terms of fundamental rights about tech companies' role in using political bots in elections?
7. Does your government protect fundamental rights against using political bots?
8. Do you know any government policy or strategies in your country against the potential impact of political bots on elections? If yes, do you think the policies or strategies are effective?
9. Have you engaged at the European policy-making level on this issue? If yes, please outline when and how?
10. To what extent do you believe the draft AI Act can meet your expectations and will it be effective?

Annex V- Interview Questions for SG3

Interview questions are prepared for the three distinct sub-groups, including

1. National Policymakers, Advisers, Rapporteurs, or Former or Current Members of the Relevant Working Groups or Relevant Institutions Across the European Union,
2. Representatives of Non-Governmental Organisations (NGOs),
3. Representatives or Staff of Companies developing AI tools

The questions in section 1 and section 2 will be directed to all interviewees. Some sub-sections are designed for specific interviewees.

The questions in sub-section 1 will be addressed to national policymakers, advisers, rapporteurs, or former or current members of the relevant working groups or relevant institutions across the European Union. The questions in sub-section 2 will be addressed to representatives of Non-Governmental Organisations (NGOs). The questions in sub-section 3 will be addressed to representatives or staff of companies developing AI tools.

COMMON SECTIONS

Common Section-1: Questions for all interviewees:

1. What is your current job title and responsibilities?
2. How long have you been working in your current job?
3. Was your previous employment experience related to technology or AI?
4. What qualifications, training or degree do you have that are relevant to your current position?
5. Are you following Artificial Intelligence (AI) technological development closely because of your job or any personal interest in AI?
6. How would you define AI?
7. Are you watching or informed on regulatory developments about AI or other new technologies?
8. Do you believe it is possible to regulate AI?
9. What do you know about bots?

Common Section-2: Questions for all interviewees:

1. What impact can AI have on the development of bots?
2. Have you ever interacted with a bot before?
3. What is your knowledge about the use of bots?
4. What do you think about the using of bots on various digital platforms such as Telegram, Slack, Twitter, and Facebook?
5. If a bot is used for political purposes, what would you think of it?
6. What is your opinion on the use of political bots in elections?
7. How do you think the use of political bots can affect the public opinion?
8. Do you think the use of bots for political campaigns or to communicate online during elections should be regulated? If yes, how should this be done?
9. Do you think that the legal documents or policies of the EU provide any protection against the use of political bots in elections?

Sub- Section 3- Questions for the Companies Developing AI Tools

1. What kinds of AI technologies does your company develop?
2. What areas/sectors are these AI technologies deployed in?
3. Are you or your company a member of any professional body that has policies related to the ethics of AI? (e.g. ACM, IEEE)
4. Do you have policies in place in your company related to the ethical and transparent design and use of AI technologies?
5. Has there been any internal training or awareness programmes to ensure employees are aware of transparency and ethical principles related to AI?
6. Have you ever worked on any political campaigns or election processes in your company or professional career? If so, could you provide some examples of the types of work that were done?
7. Can you give examples of services that are usually requested through bots and social media platforms?
8. In general, how do EU regulations affect operations or projects in your company?
9. Are you aware of EU regulations relevant to AI ?
10. What impact might the AI Act have on your company?

Annex VI - Code System

▼	 Codes	3602
>	 Demography	344
>	 Artificial Intelligence	571
>	 Bots	734
>	 Governance	1024
>	 Democracy	768
>	 Ethics	161
	 Sets	0

Annex VII - Document System

Document System		#
Documents		4090
	Sub-Group 1	1248
	SG1- Interview 1	243
	SG1-Interview 2	237
	SG1-Interview 3	242
	SG1-Interview 4	217
	SG1-Interview 5	309
	Sub-Group 2	1600
	SG2-Interview 5	296
	SG2-Interview 4	310
	SG2-Interview 3	310
	SG2-Interview 2	323
	SG2-Interview 1	361
	Sub-Group 3	1242
	SG3-Interview 5	249
	SG3-Interview 4	133
	SG3-Interview 3	232
	SG3-Interview 2	243
	SG3-Interview 1	385

Annex VIII - Detailed Code System

Code System

Code System	Frequency
Code System	3602
Demography	125
Perceptions with tech	41
Ethical concerns	4
Approach to regulations	5
Questioning approach	9
Optimism	4
Professional reasons	11
Internal concerns	7
Societal concerns	11
Sector	30
Private Sector	8
Public sector	6
NGO	17
Experience/ Years	66
Artificial Intelligence	181
Perceptions of AI	138
Economic perspective	10
Concerns about AI	29
AI as risk	70
Future risks	13
Current risks	46
Ethical risks of AI	3
Societal risks	19
Democratic risks	16
Optimism about AI	15
AI for social good	3

AI Definition	28
Bots	249
Impact on Public Opinion	72
Bot speech	2
Political bots	59
Bot Interaction	148
Dangerous	18
Legal	8
Harmless	7
Limited	19
Useful	19
Misuse of bots	12
Persuasive	6
Concern	49
Bot Detection	24
Interaction with others	8
Strengthen content	2
Content repetition	2
Bot definition	18
AI driven bots	12
Governance	272
National or supranational effects	12
Political economy	4
Other countries' approach	3
Regulatory Process	36
Measure	1
Balance	3
well-advised	3
Fragile	6
Comprehensive	9
Broad	1

Timely	3
Critical	9
Platforms	68
Future expectations	21
Expectations from new policies	8
Regulatory adaptability challenges	6
Power asymmetry	41
Platform Resistance to national/ supranational regulations	9
Regulatory power imbalance	8
Platforms as intermediaries	6
Colonialism	7
Lobbying	9
Regulatory effectiveness	73
Collaboration	1
Time lag between innovation and regulatory response	6
Overregulation	4
Representation of relevant actors	2
Governance adaptability	5
Lack of expertise	9
Enforcement challenges	19
Implementation	21
Clarity	6
Balancing innovation and regulation	12
Legal gaps	7
Regulations	115
CFR	10
Audio Visual Services Directive	1
European Media Freedom Act	2
Soft Law	5
TTPA	3
DSA	6

GDPR	9
AI Act	74
Risk-based approach	8
Perceptions on AI Act	53
Critical	28
Democracy	92
Threats to democracy	33
Political tolerance	4
Check and balance	8
Media	64
Media Influence	39
Pluralism	1
Deep fake	3
Hate speech	1
media blackout	10
Fake news	3
Misinformation	2
Disinformation	6
Media Environment	26
Elections	145
Public sphere	9
Impact on elections	31
Political bots impact on elections	17
AI impact on elections	4
Political communication	91
echo chambers	2
Manipulation	20
Computational politics	4
Political advertisement	11
Shaping public discourse	9
Micro-targeting	2

Forming public opinion	9
Political campaigns	70
Business Model	22
Promoting campaigns	15
AI driven campaigns	15
Ethics	82
Trustworthy AI	8
Robustness	1
Privacy	2
Responsibility	9
Explainability	7
Fairness	2
Accountability	14
Transparency	36

Annex IX - Memos

Code and Project Memos

Governance adaptability

Adaptiveness to current need or other countries' regulations or soft law

Demography

The code includes experience, gender, and sector information regarding the participants.

Artificial Intelligence

This code focuses on participants' perspectives on AI (includes economic perspectives, concerns, optimism, and risk-based approach) and AI definition.

Bots

This code focuses on participants' understanding of bots.

It reflects participants' bot interactions by coding them as dangerous, persuasive, limited, useful etc.

Additionally, participants' reflections on bot detection, bot definition, and AI-driven bots.

Ethics

This code categorised interviewees' reflections to ethics principles of AI such as Trustworthy AI, robustness, privacy, responsibility, explainability, fairness, accountability and transparency.

Democracy

This code is designed to cover the pillars of democracy.

It includes democracy (as a concept), media and elections.