The arrival of e-voting and campaign technologies in Europe: Promise, perils and preparedness

SUMMARY

Traditionally, political parties and electoral administrations in the European Union have been slow to adopt campaign and election technologies. However, there is now a noticeable shift among European actors towards leveraging key technologies to enhance political communication and voting procedures. Authorities in Belgium, Bulgaria, Estonia, France and one district in Portugal have already used electronic voting methods. Additionally, political parties are widely adopting data-driven campaign technology throughout Europe, including in Germany, Spain, France, Italy, Hungary, Norway and the Netherlands. Experts anticipate that political parties will further harness artificial intelligence (AI) to enhance their communication strategies.

Outlining the risks and opportunities associated with these technologies, this briefing examines how the recently updated legal framework governs content management tools utilised by political parties for the creation and dissemination of content. More specifically, it shows that political parties, intermediary services and providers of content creation solutions are subject to a range of data processing restrictions, transparency obligations and risk management requirements under the General Data Protection Regulation (GDPR), the e-Privacy Directive (e-PD), and the Digital Services Act (DSA). These obligations will become more stringent once the Regulation on the Transparency and Targeting of Political Advertising (TTPA) and the Artificial Intelligence Act (AIA) become applicable after the 2024 European Parliament elections.
Introduction

As modern technologies continue to permeate the electoral landscape in Europe, the legacy of Barack Obama’s ground-breaking presidential campaigns looms large. Often heralded as the catalyst for a technological revolution in electioneering, Obama’s strategic use of social media and sophisticated data operations set the stage for what would become known as campaign technology. However, the subsequent 2016 US presidential election and the 2017 Cambridge Analytica scandal underscored the risks associated with this digital transformation, as issues like disinformation, foreign interference, and data abuse made headlines. Today, organisations such as the International Republican Institute and the National Democratic Institute recognise both the potential benefits and pitfalls of campaign technology, offering guidance on digitising party operations.

While the US continues to be a trend-setter in campaign technology,1 accounts from Estonia, France, Germany, Hungary and the Netherlands indicate that some political parties in the EU are gradually adopting similar practices. This may be attributed to strict regulation and smaller campaign budgets. A 2021 study by the European Commission revealed that European political parties generally used online media and press as well as social media platforms, but had not adopted Artificial Intelligence (AI) and distributed ledger technologies. With the emergence of generative AI, this has likely changed in the meantime, since there are many plausible use cases, including content creation, engagement optimisation and AI-powered micro-targeting and sentiment analysis.

The above-mentioned accounts and another Commission study suggest that political parties in the EU use commercial services for targeted advertising and algorithmic segmentation. One consulting firm estimated spending of over €100 million on online political advertising in Europe in 2019. Stakeholders, especially European political parties and civil society organisations, indicated to the Commission that it was a way for them to reach potential voters and niche audiences easily, inexpensively and directly. Three relatively young parties ranked first in terms of total spending on Facebook, which supports scholars’ observations that targeted online advertising helps smaller and disruptive political parties reach wider audiences in a cost-effective way.

While there is widespread agreement that there is a transparency deficit as regards the use of targeted advertising, even less is known about political parties’ internal data processing operations, which are ‘typically shrouded in a good deal of secrecy’. Anecdotal evidence from France and a report from Hungary indicate that US practices of centralised data management and sophisticated data analytics are gradually being adopted by political parties in the EU.

Technologies in the electoral cycle

Digital technologies are playing an increasingly prominent role throughout the electoral cycle. Regulators and stakeholders usually subdivide the electoral cycle into three stages, consisting of the preparation of the election, voting and post-electoral processing. Stakeholders including Member State authorities,2 political parties, civil society organisations and private sector organisations have different roles throughout the process and make use of technologies in different ways. The focus of this section is on key technologies enhancing political communication and voting procedures.

e-Voting: Voting machines and internet voting

The COVID-19 pandemic and the need for remote voting has renewed interest in electronic voting methods. e-Voting covers the use of electronic means for the act of voting and/or counting ballots (internet voting). Internet voting, also termed ‘remote electronic voting’ and ‘online voting’, is typically conducted outside the traditional polling stations and before the traditional election days; in other words, it is a geographical and temporal remote voting option, like postal voting. In the EU, Estonia is the only country offering internet voting to all voters, whereas other countries such as France offer internet voting exclusively for voters living abroad. Several Member States also used information and communication technology solutions to send and aggregate voting tallies to
The arrival of e-voting and campaign technologies in Europe: Promise, perils and preparedness

central administrative authorities. Belgium, Bulgaria, Estonia, France and the district of Évora in Portugal have recently used e-voting; in Bulgaria, voting machines have become politically contentious. Other Member States such as Italy, Ireland and the Netherlands have experimented with e-voting, but have, for now, abandoned it.

A 2018 Eurobarometer survey revealed that e-voting is the preferred method for voting in national elections if citizens live in another EU country (42 %); ahead of voting in the embassy or consulate (27 %) or postal voting (19 %). In 2018 and 2021, the majority of respondents confirmed that they were concerned about the potential for fraud or cyber-attacks with e-voting or postal voting. In various studies and reports, the European Parliament and Commission have assessed the implications of e-voting or certain forms of e-voting such as internet/online voting. Opportunities include increased convenience and efficiency, shorter polling times, fewer counting errors, enhanced political participation and turnout, reconnecting with voters by meeting expectations regarding digitalisation, accessibility for disabled voters, crisis resilience and mitigation of risks associated with postal voting and traditional voting. Risks include technological opacity undermining accountability, erosion of trust in elections, high costs, new vectors for voter intimidation and manipulation, cybersecurity threats, less deliberation at the polling station, increased negative emotions and self-interest at voting machines, deepening of the digital divide, and reliance on the internet connections (see Annex 3).

The most recent Commission study remarks: ‘whilst no answer provided so far to try and optimise voter experience when it comes to e-voting has been totally satisfactory, this does not in any way mean that there can be no way to mitigate potential issues’. Among other things, their ‘findings exposed a paradox: although young people often ask politicians to make greater use of e-voting and social media campaigns, in practice their implementation increases negative views of politicians and heightens young people’s perceptions of a gap between themselves and the political elite’.

Some of these findings are based on observational and experimental studies, which are specific to underlying experiment design, institutional settings, legal frameworks and e-voting solutions. While negative implications appear pronounced, e-voting has also been subject to particular scrutiny compared with other forms of voting. Additionally, sociodemographic characteristics, practices, incidents and perceptions shape respondents’ experiences and attitudes. Voting methods are a habit-forming process, which may yield different results in the future.

In its 2023 e-voting compendium, the Commission highlights that ‘when implementing e-voting methods and ICT in elections, Member States should build in the necessary safeguards to ensure free, fair and resilient elections that fully uphold democratic standards and fundamental rights, including data protection and cybersecurity, as the technology evolves’. As the 2016 Parliament study states, ‘internet voting should also be relatively neutral from the political point of view, that is, the new procedure should not benefit disproportionally given factions of the political spectrum’.

Data-driven politics and campaign technology

Campaigning can be defined ‘as an organised effort, during a period before an election, where politicians try to persuade people, by influencing their decision-making process, to vote for them. In this process, different channels and media are used by political parties in order to have as wide as possible reach out to the voting audience.’ During election campaigns, candidates and political parties engage with voters to convince them of envisaged plans and policies and to win their support. Election campaigns for entering the European Parliament are largely regulated at national level. Among other things, these regulations stipulate the starting date and the length of election campaigns as well as a silence period, during which campaigning is prohibited, usually beginning 24 hours before election day and ending when the polls close.

To conduct effective campaigns and mobilise supporters, political parties increasingly rely on the support of technologies throughout the campaign. The Democratic-leaning Higher Ground Labs US venture fund has published Political Tech Landscape Reports illustrating how technology
permeates every aspect of politics (see Annex 2). Higher Ground Labs recently consulted on an AI-focused version of its annual Political Tech Landscape Report.

Data management and customer relationship management (CRM) platforms

As illustrated by Barack Obama’s 2012 presidential campaign, data and algorithms can make political campaigning much more efficient by concentrating efforts on persuadable targets. Obama’s tech, digital and analytics teams integrated scattered data sources and generated insights that helped create crucial tools such as a sophisticated email fundraising programme, a television intelligence system to guide ad purchases, and social media micro-targeting tools.

In the EU, political parties are beginning to adopt campaign technology, but little is known about specific practices. A 2016-2018 survey relating to France found that campaigners are primarily interested in less sophisticated features like emailing, contact database management, team communication, and real-time information gathering rather than data analysis and targeting techniques, which were often only used incidentally. A Human Rights Watch (HRW) report—criticised by current Hungarian State Secretary for International Communication and Relations Zoltán Kovács—found that parties across the political spectrum in Hungary invested in data-driven campaigning during the 2022 election campaign. According to the report, data collected in the course of administering public services (such as tax benefits, COVID-19 vaccines, and professional associations) was repurposed and used to disseminate ruling party Fidesz’s campaign messages. The opposition parties’ processing of personal data also lacked transparency and risked undermining privacy, but, unlike Fidesz’s data practices, HRW did not find evidence that this would create unfairness in the election process (no level playing field). German parties use CRM and targeting. Available data sources include publicly available data, inferred data, disclosed data and observed data.

Figure 1 – Functionalities of campaign technology vendors used in France

While political parties can choose from a variety of data and content management solutions, NationBuilder is used across countries worldwide and across political spectra. NationBuilder offers a suite of tools for tracking supporter behaviour, campaigning and outreach. It can be used for external-facing voter mobilisation and for organising and activating supporters. The precise classification of NationBuilder as a CRM or a data management platform likely depends on which functions customers activate and which third-party services they integrate. It has been used in France, in the United Kingdom and by the European Parliament. A request for information by the UK’s data protection authority (ICO) revealed that up to 200 political parties or campaign groups
used NationBuilder during the 2017 UK general election. Customers listed on the website include, the Austrian youth organisation Junge Linke (The Young Left), the Alliance of Liberals and Democrats for Europe Party (ALDE) and the Belgian Flemish Christian Democratic Party (CD&V).

Two of NationBuilder’s most renowned features include its database, known as ‘Nation’, and its user analytics, known as ‘Political/Social Capital’. The database serves as a centralised repository that aggregates data from across different sources and organisational units. Customers can import data on supporters from parties’ internal records, public records and marketing and online interactions. NationBuilder does not or, at least, not by default match social media accounts with email addresses of supporters registered in the database. The user analytics features are used to classify and score activity on and off the platform. Over 80 different actions influence the Political/Social Capital of supporters in the database. Political/Social Capital can be understood as a measure for engagement; it is influenced by positive interactions like donating, liking a post on Facebook or agreeing to be a fundraiser, as well as negative interactions like violating an internal rule. While NationBuilder itself relies on the Political/Social Capital indicator, some customers do not pay attention to it at all. Customers can reward positive engagement, for instance, through public leaderboards or by otherwise enhancing the social status of active supports.

NationBuilder also offers optional add-ons and possible customisation. Integrations such as Statara Solutions, Accurate Append and NamSor allow customers to append additional data to supporter files. Statara Solutions also offers ‘custom predictive models and analysis to help organisations extend their reach for recruitment, fundraising, and advocacy’. Additionally, they can integrate with data vendors through intermediaries and connect advertisement workflows with Amazon Advertising and Google Ads through intermediaries such as Pipedream and Zapier. Besides this, NationBuilder offers a Partner Portal that matches customers with partners such as RA2 consultancy – which advises inter alia on data powered campaigns – and dashboards and access to third-party data analytics and dashboard services, which can increase parties’ situational awareness and enable them to make data-driven decisions.

Online political micro-targeting

Building on the rationalisation of information, political parties rely on various forms of voter engagement, including door-to-door and digital canvassing, crowdfunding, fundraising letters, political phone banking and email marketing. Online political micro-targeting presents one of the most technically advanced and controversial practices. It involves creating finely honed messages targeted at narrow categories of voters based on sophisticated ... analysis of data garnered from individuals' demographic characteristics and consumer and lifestyle habits. It can be seen as political behavioural advertising. Under this definition, online political micro-targeting does not cover other social media activities such as sharing partisan content or posting non-personalised public posts, including by allied organisations and supporters. Voters can also be targeted through e-mails and doorstep conversations.

Online political micro-targeting gained notoriety in the wake of the Cambridge Analytica scandal. On 17 March 2018, the Guardian and the New York Times broke the story of a whistleblower claiming that his employer, Cambridge Analytica, had used 50 million Facebook profiles without users' permission, to provide data-driven services to political campaigns. Among other campaigns, the firm worked for the election teams of both former US President Donald Trump and Texas Senator Ted Cruz. The company relied on the academic work pioneered by Michal Kosinski and David Stillwell. They found, for instance, that computer-based personality judgements, based on Facebook Likes, are more accurate than those made by close contacts, such as friends, family, spouses and
colleagues. Cambridge Analytica, its former CEO Alexander Nix and app developer Aleksandr Kogan used Facebook data and results from a personality test to train an algorithm that then generated personality scores for the app users and their Facebook friends. They matched these scores with voter records for voter profiling and targeted advertising services. Cambridge Analytica explained that it used psychographic analysis to target micro-audiences with tailor-made messages appealing to these audiences. Reportedly, Cambridge Analytica oversold the size of their database and the effectiveness of their psychographic technique and micro-targeting.

The scandal culminated in a wide range of repercussions, and Cambridge Analytica filed for bankruptcy. The US Federal Trade Commission (FTC) investigated the matter and settled with Kogan and Nix on the deletion of data and business activity restrictions, and with Facebook on a penalty payment of US$5 billion and privacy restrictions. Additionally, numerous lawsuits were brought on behalf of Facebook users and consolidated into a class action lawsuit. Facebook settled with the plaintiffs on paying US$725 million and US$181 million in attorney fees. Additionally, parliamentary committees around the world, including the European Parliament's LIBE Committee and the US Senate and House Committees, organised hearings with Facebook. Despite conflicting assertions, the UK's data protection authority (ICO) controversially concluded that Cambridge Analytica was 'not involved' in the EU referendum campaign. The ICO fined Facebook GB£500 000 for failing to protect users' personal information. After the scandal, 'Facebook made changes to certain terms and policies and implemented restrictions on ... data access and sharing'.

Despite strict regulatory requirements, it is still common practice for marketers and campaigners to segment users according to demographic and custom attributes; in the EU, more so among commercial than among political actors. According to an oft-cited paper, European campaigners will not adopt political micro-targeting on a comparable scale to their US counterparts, because the European regulatory environment is stricter, most European countries follow multi-party proportional electoral systems, and political campaigns have a significantly smaller budget. Nevertheless, in several European countries, including the Netherlands, Norway, France, Italy, Spain, and Germany, academics and journalists found that political parties used targeted advertising in contemporary campaigns, but often in a less sophisticated manner than in the US or, at least, not demonstrably as sophisticated as on the other side of the Atlantic. Despite doubts regarding the effectiveness of micro-targeting, recent studies found potential, albeit limited, for persuasive returns from political micro-targeting.

Regardless of their effectiveness, non-commercial advertisers appear keen to explore targeting techniques. Assuming micro-targeting services deliver on their promises, some risks and opportunities emerge. Opportunities include enhancing voter engagement and turnout, high chances for small and new parties to gain a foothold, cost-effective and persuasive communication, mobilisation of grassroots supporters, improved voter loyalty through personalised communication, increased voter education, and feedback on voter priorities. Risks include voter manipulation, misrepresentation of political priorities, fragmentation of the political debate, ignorance of voters whose votes have minimal impact on elections, avoidance of public scrutiny, data protection and privacy violations, voter demobilisation tactics, enhancing the power of large platforms, the spread of disinformation, and the decline of traditional media (see Annex 4). Even if micro-targeting does not deliver on its promise of persuasion, it poses data protection and privacy issues and risks affecting the public sphere, including democratic institutions and processes. Scholars pointed out that the aforementioned risks may arise and intensify as a result of various factors. These include the adoption of social media of a particular design (e.g. relying on recommender systems) and a decline in solidarity, which could be linked to a significant increase in social inequality.

**AI-augmented politics and campaign technology**

As developed in a 2023 EPRS briefing, the augmentation of political and campaign technologies with AI likewise entails risks and opportunities for democracy and elections. AI can be used to
increase productivity, enhance election security and administration, **counteract** disinformation, **empower** less-resourced campaigns, enhance political advertising, moderate content, debunk fake news, **advise and educate** voters on elections and make democracy more **inclusive**. On the other hand, it may be used to create harmful content, at scale and at very low cost. Campaigners may attempt to unduly **delegitimise/disparage** rivals with realistic deepfakes, polarise and radicalise voters with disinformation, dissuade voters from participating in elections with robocalls and cloned voices (‘rumour bombing’), or avert politically damaging scandals by dismissing true information as false (‘liar’s dividend’). Additionally, AI may be used to power **political bots** that ‘astroturf’ or to facilitate **cyber-attacks** (e.g. by ‘FraudGPT’).

Amid this historic election year, AI applications have sparked fears of a big rise in disinformation. Risks arising from domestic or foreign political disinformation include societal polarisation, social unrest and **violence**, erosion of trust in democratic institutions and processes, the undermining of confidence in journalism and the media, loss of trust in science (as a spillover effect), the manipulation of elections (especially in close majoritarian voting races), discouragement of voter participation, pollution of the infosphere, content moderation that may impact freedom of expression and speech, and fact-finding inefficiencies.

The World Economic Forum (WEF) **ranked** misinformation and disinformation as the most severe risk of 2024, highlighting potential consequences such as mistrust in elections and societal polarisation. In the 2023 **Flash Eurobarometer** survey on citizenship and democracy, almost eight in 10 respondents (78%) are concerned about disinformation influencing people’s voting decisions. Another **Flash Eurobarometer**, on democracy, also published in December 2023, revealed that respondents perceive that social media are the media in which they are most likely (64%) to encounter disinformation or fake news.

The implications of disinformation, regardless of whether it was generated with the help of AI, are contentious among scholars and commentators. While some claim that disinformation does not radically change voter intentions and point out that studies often do not establish ‘reliable causal influence of fake news on voting’, others point to correlations and events that suggest a possible impact on elections and the public sphere. It should be borne in mind that neither the presence nor the absence of causality has been proven, which is unsurprising given the uncertain nature of alternative election outcomes. Although it is reasonable to guard against false narratives of stolen elections and prevent a climate of suspicion, it is equally important to take credible risks seriously. On the whole, it is worth keeping in mind that disinformation research is **becoming** increasingly **politicised**.

In the same vein, some **academics** and **journalists** challenge fears of AI-generated disinformation impacting elections as ‘overblown’. Essentially, they do not dismiss concerns, but aim to inject the debate with scepticism, encouraging reasonable reactions. Considering that widespread adoption of generative AI only began in 2022, it appears rather stringent to demand evidence of AI’s causal impact on the limited number of elections held since then. The European External Action Service (EEAS) **found** that foreign information manipulation and interference (FIMI) actors were quick to experiment with AI to generate synthetic media.

First **evidence** indicates that AI can also be used to exploit the vulnerabilities of users (possibly including susceptibility to disinformation) and influence their decision-making. AI tools may also be used to challenge technical defence measures against disinformation. In an oft-cited dystopian **thought experiment**, an AI system generates and distributes tailored messages (possibly incorporating manipulative content or disinformation) across services to sway public opinion in favour of political candidates. Ultimately, such AI systems would determine election outcomes based on technological superiority rather than on policies and debates.

The European political parties have **agreed** to abstain from producing, using, or disseminating misleading content. Many companies have signed the **AI Elections accord** seeking to combat the deceptive use of AI in 2024 elections.
The EU legal framework

The EU has taken legislative and non-legislative action to tackle risks of technology-enhanced political campaigning and communication. Most notably, the co-legislators complemented the GDPR and the e-Privacy Directive with a set of digital policies. The focus here is on the regulation of content creation and distribution, along with the tools campaigners use for such content management. The analysis accounts for the relevant parts of the TTPA and the forthcoming AIA, which will only become applicable after the 2024 European Parliament elections (Article 30(2) TTPA and Articles 113 and 111 AIA).

Limits on processing personal data in the course of content creation and dissemination

Under the GDPR, it is unlikely that campaigners could legitimately use personal details and depictions of other individuals to create and disseminate false information intended to mislead voters without consent from the data subjects concerned. Even deliberately sharing content consisting of inaccurate third-party personal data with the intention of misleading voters, while being fully aware of prior data protection violations, may be unlawful. Data protection and privacy must be balanced with the freedom of expression on a case-by-case basis. The outcome would depend on factors such as the nature of the information (e.g. opinion, opinion-related factual remark or fact statement), the sensitivity for the data subject's private life, the role played by the data subject in public life, the interest of the public in having the information, the information's framing (e.g. as a press article or scientific finding). Content that is otherwise not in compliance with EU law or the law of any Member State may not be shared (social network providers are privileged under Article 6 DSA).

Campaigners can instruct generative AI applications to generate content, including false information about third parties intended to mislead voters. Outputs can include deepfakes, fake news and cloned voice recordings qualifying as personal data. The training data, input data, output data and (arguably) even the model itself may qualify as personal data. It is not settled whether generative AI providers would qualify as controllers regarding alteration or generation of content consisting of third-party personal data. Where inputs and related outputs are processed for advertising purposes, for responding to other user's prompts ('open system'), for training the AI or for further improving services, providers may well qualify as controllers. To uphold freedom of expression and avoid over-blocking the service, they can possibly rely on 'legitimate interest' for inadvertent processing of third-party personal data submitted by (and altered upon instruction from) users. It is uncertain whether this legitimacy would depend on the adoption of organisational and technical safeguards such as ex ante reminders to respect third-party data protection and privacy rights or, controversially, ex ante filtering of evidently illegal prompts and content. This legal basis is not available for processing special categories of personal data, thus making it difficult to justify (Article 9(2) GDPR). Additionally, providers would require a legal basis for scraping and processing personal data from the internet. Further issues concerning data accuracy and the right to correction arise. The Italian Supervisory Authority went so far as to temporarily limit the processing of data by OpenAI, and NOYB recently launched a complaint against OpenAI.

It is disputed whether the GDPR applies to information disseminated at the request of the user in social networks (Article 2(4) GDPR and Article 89(2) DSA) and whether social media companies would qualify as data controllers (Articles 4(7) and 24 GDPR). Arguably, the GDPR applies and social media companies qualify as controllers, at least where they independently recommend the content to recipients and where its publication (and subsequent interactions) feeds into their advertising services. In the spirit of freedom of expression and to avoid over-blocking, inadvertent dissemination of inaccurate third-party personal data intended to mislead voters may (to a certain extent) be covered by the 'legitimate interest' legal basis. This legal basis is not available for processing special categories of personal data (Article 9 GDPR). Absent a direct relationship with
third-party non-users, consent is missing and the processing of sensitive data prima facie unlawful, unless another exception, whether written or unwritten, is found and brought to fruition. Similar issues arise where campaigners use a social media company's advertising services and that company displays the personal advertising material submitted by the campaigner to the target audience.

Additionally, controllers are obliged to take every reasonable step to ensure the accuracy of information (Article 5(1)(d) GDPR). Consequently, social media providers may have to implement notice and takedown mechanisms (see also Article 16 DSA on a compulsory notice and action mechanism for illegal content).

Data subjects can demand erasure from the social network provider pursuant to Article 17 GDPR. The right to erasure requires a delicate balance with the right to freedom of expression and information (Article 17(3)(a) GDPR). Even if freedom of expression outweighs the right to erasure, data subjects may demand correction/rectification of inaccurate personal data, 'including by means of providing supplementary statements' (Article 16 GDPR). Such a supplementary statement could provide the public with a second perspective on the information or opinion at stake. Even if the social media company qualified as a processor, it would have to assist data controllers in implementing any data subject rights exercised (Article 28(3)(e) GDPR).

Since contemporary micro-targeting implies the processing of behavioural data, including inferred and special category data, and the placing of cookies, data controllers and processors must comply with data processing restrictions contained in the GDPR and the e-Privacy Directive. The EDPB indicates that both political advertisers and social media providers offering advertising services would qualify as (joint) controllers. Arguably, social media providers can only process behavioural data for advertising purposes if they have obtained consent to do so. If the company's targeting and ad-delivery techniques rely on personal data, the accuracy of this data would likely diminish for data subjects who deny consent, and possibly overall. In the same vein, Articles 26(3) and 28(2) and (3) DSA, Article 18 TTPA and Articles 5(2) and 6(2) of the Digital Markets Act (DMA) contain further data processing restrictions that would affect targeted messaging and content dissemination.

Academics raise issues about squaring political micro-targeting and underlying ad auctions with other data protection principles, including purpose limitation, data minimisation, accuracy, accountability and integrity, and confidentiality (Article 5 GDPR and their various expressions in the Regulation). The fairness principle under Article 5(1)(a) GDPR likely prohibits processing behavioural data to manipulate data subjects, and possibly unreasonably contributing to this by processing data as part of advertising services that are inherently prone to misuse for such purposes.

Limits on the design and use of content management systems

AI systems that distort a person's behaviour in a significantly harmful manner by deploying subliminal or purposefully manipulative techniques or exploiting vulnerabilities (possibly as part of a political advertisement or a disinformation campaign) are prohibited (Articles 5(1)(a) and (b) AI). Among many unsettled issues, the question arises as to whether only specialised systems, which the provider intentionally designed to deploy manipulative techniques, are prohibited, or also systems that systematically or incidentally manipulate or deceive in pursuit of their encoded (lawful) objectives. In the same vein, it is questionable whether AI systems 'deploy purposefully manipulative or deceptive techniques' where providers design a system that (foreseeably) allows users to configure the system so that it serves manipulative content to vulnerable individuals (e.g. by using AI-powered targeting and ad-delivery techniques).

Online platforms must facilitate changing the relative order displayed to recipients where they provide recipients with the options to modify parameters used in recommender systems (Article 27(3) and Recital 70 DSA). Very large online platforms (VLOPs) and very large online search engines (VLOSEs) must provide at least one option for each of their recommender systems that are not based on profiling (Article 38 and Recital 94 DSA).
Transparency obligations regarding content management

A wide range of transparency obligations apply, which holds potential for public oversight:

- Where the presentation of an advertisement qualifies as an automated decision within the meaning of Article 22 GDPR, data subjects would (among other things) likely have a right to an explanation of the decision (Articles 15(1)(h), 14(2)(g), 15(1)(h) and 22 GDPR).

- The DSA imposes varying degrees of transparency obligations on intermediary services. They must inform recipients, authorities and vetted researchers about certain features of their services, including advertising and recommender systems. They must include information on content restrictions, content moderation and recommender systems in their terms and conditions (Articles 14, 23(4) and 27 DSA). They must publish content moderation reports (Articles 15, 24(1) and 42(1)-(3) DSA) and information on the average monthly active recipients (Article 24(2)-(4) DSA). Online platforms must inform recipients of certain advertisement features, including the main parameters determining to whom the advertisement was presented and how recipients can change the parameters (Article 26(1) DSA). VLOPs and VLOSEs need to maintain a public repository of advertisements published and include the main targeting parameters (Article 39 DSA). Upon a reasoned request from the Digital Services Coordinator, VLOPs and VLOSEs must grant vetted researchers access to data necessary for monitoring and assessing compliance (Article 40(4) DSA).

- Chapter II TTPA contains a wide range of transparency obligations for providers of political advertising services, including for publishers. Crucially, publishers must inform users, authorities and interested parties about features of the political advertising. For instance, political advertising must be labelled as such (Articles 11 and 19 TTPA), accompanied by information on the targeting and ad-delivery techniques (Article 12 TTPA) and submitted to a public repository for online political advertisement (Article 13 TTPA). Data controllers are subject to additional transparency requirements as regards targeting and ad-delivery techniques (Article 19 TTPA). Upon request, certain data must be shared with interested parties, including vetted researchers, members of civil society organisations, and journalists (Articles 17 and 20 TTPA).

- Gatekeepers must provide publishers and advertisers with access to performance measuring tools or to the necessary data (Article 6(8) DMA) and publish annually an overview of independently audited descriptions of profiling techniques used on consumers across its core platform services (Article 15 DMA).

- Providers of high-risk AI systems, presumably including AI-powered advertising systems intended to influence the outcome of elections or relying on certain biometric data processing, would need to submit a description of the information used by the systems and its operating logic to a public repository of high-risk AI systems (Articles 49(1) and 71(2) and Annex VIII, point 1 AIA). Deployers must inform individuals about the use of high-risk AI systems for decision-making or assisting with decisions (Article 26(11) AIA). Citizens will have a right to an explanation of individual decisions based on high-risk AI systems that affect their rights (Article 86 AIA).

- Providers of AI systems generating synthetic content must ensure that the generated synthetic output is (machine-readably) marked as artificially generated or altered (Article 50(2) AIA). Deployers of AI systems capable of generating synthetic content must disclose that deepfakes and manipulated public information texts have been generated artificially, unless freedom of speech requires an exception to this obligation (Article 50(4) AIA). Providers of proprietary general-purpose AI models must make publicly available a sufficiently detailed summary of the content used for the training of their general-purpose AI (GPAI) model (Article 53(1)(d) AIA). Providers of AI systems intended to interact with natural persons, such as political (chat)bots, must inform individuals that they are interacting with AI systems (Article 50(1) AIA). Finally, deployers must inform individuals concerned about the operation of any emotion recognition or a biometric categorisation system (Article 50(3) AIA).
Risk management requirements regarding content management

Additionally, several digital policies prescribe risk management duties. For processing that is likely to result in a high risk for individuals, data controllers must perform a data protection impact assessment (Article 35 GDPR). The impact assessment must consider the risks to the rights and freedoms of natural persons, primarily to data protection and privacy, but arguably also freedom of speech, freedom of thought, prohibition of discrimination, and the right to liberty, conscience and religion (Article 35(7b) GDPR). To avoid having to consult the supervisory authority, they would need to mitigate any high risks prior to processing the data (Articles 35(7)(d), 36 and 25 GDPR).

VLOPs and VLOSEs must assess systemic risks arising from their services and systems and put in place proportionate mitigation measures. They must account for systemic risks such as the dissemination of illegal content, negative effects on the exercising of fundamental rights, negative effects on civic discourse and electoral processes, and how factors such as algorithmic systems (including recommender systems), content moderation systems, advertising systems and possible intentional manipulation of their services influence the systemic risks (Article 34 DSA). Mitigation measures may include adapting their terms and conditions, the functioning of the service, content moderation processes, algorithmic systems (including recommender systems), and advertising systems, as well as ensuring that false information is marked (Article 35(1)(a), (c), (d), (e) and (k) DSA).

Providers must set up a quality management system for high-risk AI systems, which provides for, among other things, ex ante testing, systems and procedures for data management, a risk management system, a post-market monitoring system, and procedures for record-keeping (Articles 16(c) and 17 AIA). The risk management system requires the iterative identification and analysis of known and reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights, as well as the adoption of appropriate and targeted risk mitigation measures (Articles 17(1)(g) and 9 AIA and Recital 65 AIA): ‘This process should ensure that the provider identifies risks or adverse impacts and implements mitigation measures for the known and reasonably foreseeable risks of AI systems to the health, safety and fundamental rights in light of their intended purpose and reasonably foreseeable misuse, including the possible risks arising from the interaction between the AI system and the environment within which it operates’ (Recital 65 AIA). Where campaign technology incorporates AI systems intended to be used for influencing the outcome of an election or relies on certain biometric data processing, risks of privacy intrusions, biased results, discriminatory effects and adverse effects on democracy and the rule of law must be assessed and mitigated (Recitals 54-62 AIA).

Providers of GPAI models with high-impact capabilities, such as ChatGPT-4, must assess and mitigate possible systemic risks (Article 55(1)(b) AIA). Systemic risks include any actual or reasonably foreseeable negative effects on democratic processes and the dissemination of illegal, false, or discriminatory content, as well as privacy harms (Recital 110 AIA). Providers ‘should continuously assess and mitigate systemic risks, including for example by putting in place risk-management policies, such as accountability and governance processes, implementing post-market monitoring, taking appropriate measures along the entire model’s lifecycle and cooperating with relevant actors along the AI value chain’ (Recital 114 AIA). Where VLOPs or VLOSEs embed such systems and meet the DSA’s risk management requirements, it should be presumed that they meet the corresponding obligations under the AIA, unless significant systemic risks that are not covered by the DSA are discovered (Recital 118 AIA).

Many details regarding the application of these new laws remain unsettled, and academics have begun identifying outstanding gaps in protection. Other rules such as the Audiovisual Media Services Directive (AVSMD) and national rules may apply. Customer relationship and data management systems as well as e-voting solutions must also comply with a range of obligations, including data protection and cybersecurity requirements.
ENDNOTES

1 Democrats and Republicans have both launched incubators to fund the future of campaign technologies. Additionally, the ‘Tech for Campaigns’ platform enables volunteers to support campaigns of Democrats in 6-8 week-long tech projects. The CampaignTech Innovation Summit lists topics such as AI, post-cookie advertising, virtual voter contact, emerging platforms, analytics and targeting as campaign-defining topics.

2 In a 2021 Commission study, few EU Member State authorities confirmed using technologies for registering voters and political parties, gathering information or approving candidates’ lists. The use cases annexed to the study revealed that authorities used technologies to support activities such as nominating election committee members, registering candidates, preparing polling cards, voting electronically, counting votes, publishing results and preparing statistical reports. A 2020 Council of Europe report on digital technologies in elections contains examples.

3 The European Data Protection Supervisor (EDPS) issued a reprimand to the European Parliament for contravening the GDPR by using NationBuilder in its public engagement campaign thistimeimvoting.eu ahead of the 2019 European Parliament elections. Parliament deleted the data from over 260,000 users who had not accepted an updated privacy policy out of data collected from more than 329,000 users.

4 Previously, NationBuilder offered the NationBuilder Match feature, which automatically retrieved certain social media information of supporters added to the database. Reportedly, this included, for some social networks, location and biography data. NationBuilder also provided for the possibility of adding all internet users who had liked a candidate’s post on Facebook or followed him or her on Twitter to the database. The Match feature had been enabled by default since 2013. After the French data protection authority (CNIL) raised concerns about the matching capabilities, NationBuilder deactivated the Match functionality by default in France, and subsequently across all EU Member States. Besides this, it is worth noting that NationBuilder now offers ‘Advanced Privacy tools’.

5 See Article 3(2) and (11) Regulation (EU) 2024/900 (TTPA) for a legal definition.

6 Although the Court approved the settlement, pay-outs are precluded by appeals by three Facebook users who objected to the settlement.

7 The International Institute for Democracy and Electoral Assistance notes: ‘In proportional systems, micro-targeting might have more difficulty yielding impactful results as tapping into a small segment of the population can only have marginal effects on the total count of votes. However, a significant micro-targeting campaign directed to the right sectors of society might be able to tip the balance of an election’.

8 Account verification and verifiable content signing may help mitigate such risks.

9 Anecdotal evidence indicates that well-timed, last minute disinformation campaigns reach voters and can impact elections, especially when media outlets and politicians must avoid election-related (possibly corrective) announcements due to silence periods.

10 They might publish either as users, directly uploading harmful content to the platform, or as advertisers, utilising advertising services to disseminate the disinformation. For the GDPR to apply, the campaigners must use automated means (Article 2(1) GDPR).

11 Private users would benefit from the household exemption under Article 2(2)(c) GDPR.

12 It is unsettled whether this legitimacy would depend on the adoption of reasonable organisational and technical safeguards such as ex ante reminders to respect third party rights, ex post notice and takedown procedures, or even ex ante filtering of evidently illegal content. In a different yet related context, Advocate-General Szpunar considered that ex ante filtering is not desirable.

13 A preliminary ruling of the Court of Justice of the EU (CJEU) rendered the consent management platforms used to obtain consent to be non-compliant. In a recent opinion, the European Data Protection Board (EDPB) held that large platforms such as Instagram and Facebook do not meet GDPR consent requirements if they offer users a choice between consenting and paying to avoid targeted advertising.

14 Facebook and Google review advertisements before publishing them.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2024.

Photo credits: © Maxim Basinski / Adobe Stock.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)
## Annexes

### Annex 1: Official guidance documents

<table>
<thead>
<tr>
<th>Category</th>
<th>Documents</th>
</tr>
</thead>
</table>
| **General**    | • European political parties, [Code of Conduct](#) for the 2024 European Parliament elections, 9 April 2024 [background policy brief].
|                | • EDPB, [Statement 2/2019](#) on the use of personal data in the course of political campaigns, 13 March 2019 (Annex I refers to guidance from data protection authorities).  
|                | • EDPB, [Guidelines 8/2020](#) on the targeting of social media users, 13 April 2021.  
|                | • Council of Europe, [Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns](#), February 2022.  
|                | • Global Privacy Assembly (International Conference of Data Protection and Privacy Commissioners), [Resolution on the Use of Personal Data for Political Communication](#), 2005. |
| **Content**    | • Commission [communication](#) on tackling online disinformation: a European Approach, COM(2018) 236 final, 26 April 2018.  
|                | • Commission [guidance](#) on strengthening the industry [code of practice](#) on disinformation, COM(2021) 262 final, 26 May 2021 (measures planned to protect the European elections 2024).  
|                | • Commission [guidelines](#) for Providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes, C(2024) 2121 final, 26 March 2024.  
|                | • Commission [Recomendation 2018/334](#) on measures to effectively tackle illegal content online.  
|                | • The EU [Code of Conduct](#) on countering illegal hate speech online, 30 May 2016.  
|                | • Council of Europe [recommendations and guidance](#). |
| **Infrastructure and integrity** | • Commission [communication](#) on defence of democracy, COM(2023) 630 final, 12 December 2023.  
|                | • Commission [recommendation 2023/2829](#) on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament, 20 December 2023.  
|                | • [Compendium](#) on elections cybersecurity and resilience, as updated on 6 March 2024.  
|                | • [Compendium](#) of e-voting and other ICT practices, non-paper, 6 December 2023.  
|                | • CNIL, [Délibération n° 2019-053](#) portant adoption d’une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet, 25 April 2019.  
|                | • Council of Europe [recommendations and guidance on e-voting](#). |

Data source: Author's own compilation, May 2024.
Annex 2: 2022 Political Tech Landscape Report

Source: Higher Ground Labs [website](https://highergroundlabs.org).
Annex 3: Risks and opportunities of e-voting

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Increased convenience and efficiency:</strong> e-voting offers increased convenience by allowing voters to cast their ballots from anywhere with internet access. This efficiency can lead to quicker vote tallying and result reporting.</td>
<td><strong>Reduced accountability:</strong> The transmission of electronic ballots is often hidden from the public eye, creating concerns about accountability and transparency.</td>
</tr>
<tr>
<td><strong>Shorter polling time:</strong> Electronic voting reduces the time needed to cast a vote, resulting in shorter stays at polling stations.</td>
<td><strong>Self-interest voting increased:</strong> Voters using electronic methods are less likely to consider the broader national interest and more likely to vote based on personal gain. This can skew election outcomes towards individual rather than collective benefits.</td>
</tr>
<tr>
<td><strong>Reconnecting with voters:</strong> In a context of growing dissatisfaction with politics, internet voting can help reconnect voters by offering a modern and accessible voting method. This approach can engage younger and more tech-savvy citizens.</td>
<td><strong>Increased negative emotions:</strong> Some citizens experience negative emotions such as worry and nervousness when using voting machines. This can affect their voting experience and satisfaction with the process.</td>
</tr>
<tr>
<td><strong>Increased democratic participation:</strong> e-voting facilitates broader participation of citizens living abroad and disadvantaged groups.</td>
<td><strong>Mixed turnout implications:</strong> Turnout among young people may be lower for electronic voting compared to traditional polling stations. Polling station voting reinforce group dynamics about political participation, and the implications of remote voting on overall turnout are mixed.</td>
</tr>
<tr>
<td><strong>Accessibility for disabled voters:</strong> e-voting increases accessibility for disabled voters by offering assistive technologies. This ensures that all citizens, regardless of physical ability, can participate in the electoral process.</td>
<td><strong>Inadequate disability accommodation:</strong> e-voting methods do not always sufficiently accommodate different disabilities. This can exclude some voters from participating fully in the electoral process.</td>
</tr>
<tr>
<td><strong>Fewer counting errors:</strong> Electronic voting reduces the risk of human error in vote counting, leading to more accurate election results. Automated systems can handle large volumes of votes more efficiently than manual counting.</td>
<td><strong>Loss of integrational moment:</strong> Internet voting can eliminate a key moment of integration and equality for vulnerable citizens. Traditional polling stations provide a communal experience that can foster social inclusion.</td>
</tr>
<tr>
<td><strong>Cost-effective:</strong> Over time, e-voting can be cost-effective by reducing the need for physical polling stations and printed ballots. The initial investment in technology can be offset by long-term savings in operational costs.</td>
<td><strong>Less deliberation:</strong> Voters take less time to deliberate when using voting machines. Quick voting can diminish the sense of importance and reflection associated with casting a ballot.</td>
</tr>
<tr>
<td><strong>No dependency on postal services:</strong> e-voting eliminates the dependency on postal services, reducing the risk of late arrival of votes.</td>
<td><strong>Higher costs:</strong> Currently, voting machines incur higher costs than traditional paper ballots. The initial investment in technology and maintenance can be significant.</td>
</tr>
<tr>
<td><strong>Low security risks:</strong> Genuine security risks of electronic voting machines are not particularly high and can be effectively mitigated through robust cybersecurity measures. Continuous advances in technology enhance the security of electronic voting systems.</td>
<td><strong>New vectors for voter intimidation and manipulation:</strong> Remote voting increases the risk of voter intimidation and manipulation, as ballots can be cast in uncontrolled environments. This undermines the privacy and independence of the voting process.</td>
</tr>
<tr>
<td><strong>Crisis resilience:</strong> e-voting serves as a viable solution during crises, such as pandemics or natural disasters, where physical polling stations may be unsafe or impractical. This ensures continuity in the democratic process.</td>
<td><strong>Cybersecurity threats:</strong> Concerns over security threats and potential tampering persist with electronic voting. Ensuring the cybersecurity of voting systems remains a critical challenge.</td>
</tr>
<tr>
<td><strong>Vulnerable to legitimacy attacks:</strong> Due to general scepticism, it is easier to cast suspicion on the integrity of the electoral process with electronic voting. This can threaten the credibility of election results and public trust in the democratic process.</td>
<td><strong>Deepening of the digital divide:</strong> Electronic voting may deepen the digital divide, disadvantaging those without access to technology or the internet. This can lead to unequal participation and representation.</td>
</tr>
<tr>
<td><strong>Reliance on internet connections:</strong> e-voting systems are reliant on stable internet connections, which can be a limitation in areas with poor connectivity. Interruptions or outages can disrupt the voting process.</td>
<td></td>
</tr>
</tbody>
</table>
### Opportunities

**Enhanced political pluralism:** Targeted online advertising allows small and new parties to allocate their resources efficiently towards seeking supporters and building a platform. This may strengthen political pluralism, representation and participation.

**Improved voter turnout:** Micro-targeting can help identify potential voters who are likely to support a candidate but may not be planning to vote. Targeted messaging and reminders can encourage these individuals to turn out on election day.

**Customised policy communication:** Campaigns can use micro-targeting to communicate policy positions that resonate with specific voter segments. This ensures that voters receive information on issues that matter most to them, increasing the likelihood of support.

**Increased voter education:** Targeted efforts can provide voters with relevant and detailed information about candidates and their platforms. This helps voters make more informed decisions at the polls.

**Better understanding of the electorate:** By understanding the priorities of different voter groups, campaigns can emphasise issues that are most likely to attract support. This strategic focus can strengthen the campaign’s appeal and voter alignment.

**Improved voter loyalty:** Personalised communication can foster a stronger connection between the candidate and the voter. This relationship-building can increase voter loyalty and long-term support for the candidate or party.

**Increased persuasion:** Tailored messaging can address the specific concerns and interests of different voter groups, making the campaign’s arguments more persuasive. This targeted approach can be more effective in swaying undecided voters.

**Efficient resource allocation:** By identifying and targeting key voter segments, campaigns can allocate their resources more efficiently. This ensures that time and money are spent on reaching the most influential and persuadable voters.

**Enhanced grassroots mobilisation:** Micro-targeting can identify and activate supporters who are willing to volunteer and advocate for the campaign. This grassroots mobilisation can amplify the campaign’s reach and impact.

### Risks

**Voter manipulation:** Political campaigns may manipulate voter views and behaviour by exploiting individual vulnerabilities and triggering unconscious cognitive processes through personalised designs and deceptive ads. This can lead to elections being decided by financial resources and social engineering rather than genuine political considerations. Campaigners would rely on correlations to target persuadable voters rather than addressing views, values, needs or desires and engaging in a public debate/deliberative processes on the substance.

**Misrepresentation of political priorities:** Voters might overestimate the importance of certain topics because personalised ads lack the context of mass messaging. Due to the insular consumption and transient nature of micro-targeted ads (‘dark ads’), campaigners may even send irreconcilable or divisive messages to different targets that would otherwise be rejected by the public. Some experts criticise the fact that the mandate of elected officials is weakened since voters decide based on a patchwork of discrete issues.

**Fragmentation of public discourse:** Micro-targeting can create echo chambers, leading voters to focus solely on their concerns and fostering polarisation. This diminishes the shared reality needed for mutual understanding and compromise in politics. However, an oft-cited paper posits that voters do not live in political digital bubbles. Another paper suggests that polarisation can also result from offline factors, such as the decline in solidarity, possibly driven by a significant increase in social inequality.

**Exclusion of certain voter groups:** Voter groups that are not relevant to win elections (e.g., non-voters or firm supporters) might be ignored by political campaigns and therefore excluded from democratic deliberations (political red-lining).

**Less oversight:** Due to the insular consumption and transient nature of micro-targeted ads, advertising may avoid stringent oversight and scrutiny by the public, press, researchers and regulators. Due to limited reputational risks, the need for brand safety may exert less self-regulatory pressure on publishers.

**Concealment of advertisers’ identity:** Political advertisers can avoid legal and reputational accountability by hiding their identities. This lack of transparency undermines the integrity of political advertising.

**Challenges to electoral rules:** Political micro-targeting practices challenge established electoral rules concerning transparency, campaigning and political funding.

**Privacy concerns:** Ubiquitous tracking, identifier matching, data integration from different sources, data sharing with the digital advertising supply chain and psychographic profiling may go beyond reasonable expectations of data subjects and lack legal bases under the GDPR.

**Chilling effect on freedom of expression:** Users may hesitate to express their opinions online or seek out certain information due to concerns over political tracking and profiling driven, inter alia, by the data needs of online political micro-targeting.

**Reluctance to vote:** Where political parties use the electoral roll (voter list) for campaigning and micro-targeting, voters may be reluctant to register and vote due to the undesired secondary data processing.
### Opportunities

#### Risks

**Increased power of large platforms:** Political micro-targeting through large platforms such as Google and Meta may further increase their already significant power in the social media, publishing and adtech markets.

**Gatekeeping:** The near-monopoly position of large platforms raises the risk of them becoming gatekeepers, influencing politics and setting prices (price makers). This may come in different forms – for instance, preferential access to data or preferential dissemination of content. Their ability to determine the user’s exposure to content gives them great power.

**Spread of disinformation:** Partisan actors may exploit advertising services to disseminate disinformation, fake news, conspiracy theories, inflammatory content and hate speech for political gain. While the effect on voter behaviour appears small, it may exacerbate existing beliefs, spur polarisation and affect social cohesion. Arguably, using political micro-targeting services feeds into an ecosystem that algorithmically amplifies fake news and divisive content, to draw attention so that it can sell advertising space (ad-driven content). The algorithms are optimised to increase ad revenues.

**Voter demobilisation tactics:** Political rivals may discourage voters from participating in elections – for instance, by framing the rejection of voting as an act of resistance (‘hyperlocal voter suppression’).

**Accessibility issues for small parties:** Certain forms of sophisticated targeting may be prohibitively expensive and therefore inaccessible to small parties. This may tilt the public discourse in favour of wealthy political actors.

**Decline of traditional media:** As traditional media outlets lose advertising revenue to social media platforms, there is a decline in traditional media outlets and journalistic norms of impartiality, accuracy, accountability, etc. are lost.

---

Data source: Based on sources linked in the table and the text.