
# TECHNOLOGY, DATA AND ELECTIONS: A checklist on the election cycle

November 2023

privacyinternational.org

# ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.



Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Cover image: Photo by Kvistholt Photography on Unsplash

## Introduction

In the last few years, the issue of data in elections has increased in visibility and profile. Now more than ever, there is an acknowledgment of the pivotal role that data can play in electoral processes and the diversity of the actors involved in data processing activities.

The ability to harness and analyse vast troves of personal data has redefined political campaigning and enabled the proliferation of political advertising tailor-made for audiences sharing specific characteristics or personalised to the individual. These new practices, combined with the platforms that enable them, create an environment that facilitate the manipulation of opinion and, in some cases, the exclusion of voters.

In parallel, several states are turning to biometric voter registration and verification technologies ostensibly to curtail fraud and vote manipulation. The resulting modernisation of the electoral infrastructure is often accompanied by the development of nationwide databases containing masses of personal, sensitive information, that require heightened safeguards and protection. Often, the increased reliance on technologies for purposes of voter registration and verification goes hand in hand with the involvement of private companies, a costly investment that is not without risk.

This new electoral landscape comes with many challenges that must be addressed in order to protect free and fair elections: a fact that is increasingly recognised by policymakers and regulatory bodies. In recent years, this has prompted a surge in regulatory efforts aimed at ensuring transparency, accountability and the ethical use of data in electoral activities. These have ranged from investigations and the issuance of guidelines by international and domestic bodies to new legislation aiming to set limits on the use of data for political campaigning purposes. Despite these initiatives, the use of data in electoral context remains unregulated in many jurisdictions.

This rapidly evolving and intricate environment requires experts and monitors to grapple with the relationship between data, technology and elections. Electoral observers can play a pivotal role in bridging the current knowledge gap that often exists between the public and government officials on this relationship, bolstering voters' trust in the electoral process by providing an independent, impartial, and expert assessment of all the relevant aspects of the electoral process. By incorporating methodologies which consider the role of electoral technologies and data, observers can provide recommendations on how to effectively respect and protect privacy in the entire electoral cycle.

This updated data and elections checklist aims to provide electoral observers and interested members of civil society with the relevant tools to examine and unpack some of the most complex and challenging aspects of the electoral process as they pertain to data and technology.

Throughout this checklist, Privacy International identifies the main areas where technology and the processing of personal data intersect to play a key role in the electoral process. The briefing is structured to follow the methodologies developed by election observer organisations. Each section offers a brief description of the issue at stake, policy recommendations, and key questions that election observers could use to assess whether the national framework is adequate to protect against the exploitation of data in the electoral process. These questions are intended as a starting point in the analysis.

The first part covers the overarching legal framework and the relevant regulations related to the administration of elections, as well as the role of third-parties playing a role in the provisioning or management of electoral technology (voter registration, voting, the role of the Electoral Management Body and private companies.) The second part examines the regulation of political parties and other political actors (including financing and political campaigns.) The third part focuses on the role of online platforms, notably search engines and social media platforms, in the context of elections (with particular focus on transparency of political advertising.)

## Part 1 – Administration of the Elections

### 1.1.Legal Framework – protection of the right to privacy in the electoral process

The right to privacy (Article 17 of the International Covenant on Civil and Political Rights, ICCPR) is a fundamental human right, which is significantly and increasingly relevant in the election context.

As noted by the Council of Europe, the protection of privacy in political campaigns is crucial to the conduct of fair and free elections.[1] In this context, the right to privacy is understood to guarantee the citizen's free expression, the proper representativeness of elected representatives and the legitimacy of the legislative and executive bodies, and by the same token enhances the people's confidence in institutions.[2]

The protection of personal information is inextricably linked to the right to privacy, as noted by the UN Human Rights Council in October 2023.[3] The Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns adopted by the Council of Europe in November 2021 note that "as elections in most countries have become increasingly "data-driven," it is therefore critically important that all organisations involved in political campaigns process personal data on voters in compliance with well-established data protection principles".[4]

As noted by the European Commission and the Council of Europe respectively, data protection is necessary for democratic resilience[5] and the application of sound data protection principles contributes to strengthening the integrity of elections and maintaining trust in democracy in the digital age.[6]

To date, 137 countries around the world have enacted data protection laws.[7] However, these laws are often out of date, not comprehensive (notably they often exclude the processing of

[1] Introduction, the Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns.
[2] Ibid.
[3] U.N. Doc. A/HRC/54/L.12/Rev.1, 9 October 2023.
[4] Introduction, the Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns
[5] See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0638
[6] Introduction, the Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns
[7] As of October 2020, see Data Protection and Privacy Legislation Worldwide, available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

personal data by public authorities) and lack independent oversight and redress mechanisms.[8] Data protection laws may also include exemptions for political parties that risk facilitating data exploitation during political campaigns.[9] Such laws should be assessed and updated as necessary.

The right to privacy is also an enabling right, permitting the enjoyment of other human rights, most notably, in the context of elections and political campaigning, the right to freedom of expression (Article 19 of ICCPR) and the right to political participation (Article 25 of ICCPR). The right to privacy enables the capacity of individuals to form opinions, including political opinions, without undue interference.

The UN Human Rights Committee interpreted the right to political participation under Article 25 of ICCPR to encompass that "voters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind". The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has gone further, noting there is a real concern that the systematic collection of data about users' activities online and targeted advertising may violate their right to freedom of opinion under Article 19 of the ICCPR.[10] In particular, she states that techniques such as content moderation and microtargeting play a significant role in spreading disinformation and, as involuntary or non-consensual manipulation of thinking processes, contravene the right to freedom of opinion.[11]

**Recommendations**

- National laws, ideally the Constitution, should recognise the right to privacy, including the protection of personal data.
- A modern, comprehensive data protection law should be in place with an independent, adequately resourced data protection authority, with powers to investigate, receive complaints and impose sanctions. The law should be regularly reviewed to ensure its provisions are up to date and effective in addressing the challenges posed by the application of new technologies, including in the electoral context.
- The national data protection authority should issue a Code of Practice or equivalent, or at the very least guidance on the use of personal data in the electoral process, highlighting the data protection obligations of all actors involved in the electoral process, including political campaigns.

**Questions**

- Does the constitution or other legislation protect the right to privacy, including the protection of personal data?
- Is there modern, comprehensive data protection legislation? Does it cover processing of personal data by public authorities?
    - Does it have exemptions for political parties or other campaign actors?

[8] Privacy International has developed a guide on data protection legislation, which identifies relevant international and regional standards and best practices: https://privacyinternational.org/type-resource/data-protection-guide

[9] See: https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation-political-parties

[10] U.N. Doc. A/HRC/47/25, para. 66, 13 April 2021. Available at: https://www.ohchr.org/en/calls-for-input/report-disinformation

[11] Ibid., para. 36.

    - Does it establish an independent national data protection authority?
- If there is a national data protection authority, has it issued guidance on the use of personal data in the electoral process?
    - Does the guidance or other data protection framework for political activities:
        - Include a broad definition of political campaigning?
        - Apply beyond political parties to other important actors, such as the electoral management body, platforms and data brokers?
        - Interpret personal data broadly, to include what is derived, inferred and predicted (as the results of profiling)?

### 1.2. Voters' registration

Voters' registration is necessary for the effective functioning of elections. It aims at ensuring and enabling the voting of only those eligible to vote. Hence it relies on some form of verification of someone's identity against a voters' registry or electoral roll. Only the personal data necessary to identify a voter and establish eligibility to vote should be recorded.

Similarly, access to the voters' register by actors monitoring the election and by political parties is necessary to safeguard the fairness of the electoral process and to reach out to potential voters, but it should not lead to unfettered access. Lastly, even when the personal data contained in the personal register is made public, any use of such personal data should be subject to data protection safeguards.

While the setting up of voters' registers varies from country to country, increasingly governments are creating centralised databases which store a vast array of personal data about voters, sometimes including biometric data. It is now common that voter registration data is kept in a central, electronic database. While this has its advantages, particularly in relation to improving transparency and responsible access to and sharing of the data, centralised electronic registers raise concerns related to the safety of the personal data stored and the possible misuse of the data.

In fact, if not properly regulated, these voter registers may undermine the democratic processes they ostensibly support.

First, personal data contained in these databases might be combined with other data and used for profiling of potential voters in ways that seek to manipulate their opinions. This issue is also addressed in section 2.2 below.

In Kenya during the 2017 presidential election, there were reports that Kenyans received unsolicited texts messages from political candidates asking the receiver to vote for them.[12] These messages referenced individual voter registration information such as constituency and polling station, which had been collected for Kenya's biometric voter register. Concerns remain that this database was shared by Kenya's electoral commission (IEBC) with third parties, without the consent of the individual voters, and that telecoms companies may have shared subscriber information, also without consent, in order to allow this microtargeting to happen.

[12] See https://sur.conectas.org/en/a-very-secret-ballot

It is not clear who the registration database was shared with and therefore which company, if any, was responsible for this microtargeting. In the 2022 elections, these concerns resurfaced when the IEBC announced the sale of the voter register for a "fee".[13]

Second, while political parties have a legitimate interest in accessing personal data contained in the voter register, this should not result in unfettered access and use of such data. Who has access to the data and for what purposes should be prescribed by law.[14]

In some countries there will be two registers, a general register (with access restricted by law) and an edited or open register (which anyone can buy access to). In the UK,[15] for example, the general (full) register is available to those prescribed by law, such as electoral registration officers, registered political parties, candidates, local authorities and credit reference agencies. They should only be able to use the data for specific purposes also prescribed by law. The edited/ open register (which operates on an opt-out basis), can be bought by anyone and used for a wide range of purposes. Therefore, an entity with access to the full register is not permitted to share it without a lawful basis. For example, a credit reference agency should not share this data with other data brokers for marketing purposes.

Third, lack of adequate security of the electoral register might also result in data breaches or leaks of personal data, which might discourage voters from registering in the first place and could lead to other harms such as identity theft.

Lack of adequate security has resulted in unauthorised data access of millions of people in countries across the world. In March 2016, the personal data of over 55 million registered Filipino voters was leaked following a breach on the Commission on Elections' (COMELEC's) database,[16] which the national data protection authority concluded had granted access to both personal and sensitive data. In August 2023, it emerged that a hostile cyber-attack targeting the full electoral register in the UK had resulted in the unauthorised access to the data of 40 million voters, including their names and addresses.[17] It later emerged that the Electoral Commission had failed a basic security test around the time its registers were hacked, calling into question the effectiveness of safeguards in place at the time.

[13] Privacy International, Our final report on Kenya's 2022 election in collaboration with The Carter Center Election Expert Mission, 21 March 2023. Available at: https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert

[14] As noted by the CoE in its Guidelines on the Protection of Individuals with regard to the Processing of Personal Data: "Where political campaign organisations legally acquire the official voters list from the election regulatory body to assist their campaigns, the law should stipulate who is entitled to access these data, and for what purposes, limited to what is necessary for engaging with the electorate with clear prohibitions and appropriate sanctions for using the data for any other purposes."

[15] See: https://ico.org.uk/your-data-matters/electoral-register/

[16] See https://www.privacyinternational.org/state-privacy/1009/state-privacy-philippines

[17] See https://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems

**Biometric voter registration (BVR)[18]**

Proponents of BVR argue that it is effective against voter fraud, such as voter impersonation and multiple voting. However, BVR cannot fully replace other mechanisms to ensure the voters' register is up-to-date (e.g. reporting deceased registrants and removing them for the register.) In addition, BVR brings specific challenges relating to the costs of the technology, its maintenance and its support (which can in turn raise risks of corruption or, for developing countries, donor dependency.)[19]

BVR can be used for deduplicating the voter roll, and/or for verifying the identity of a voter when they are at the polling station. The consequence of using biometrics for this purpose is a centralised database of the biometrics of the entire population on the roll. The BVR should embed privacy by default and by design. For example, a system of authentication designed purely for de-duplication does not have to link the biometrics in any way to the individual; all it needs to know is whether it has seen these particular biometrics before (i.e., answering the question "is this an eligible voter?", as opposed to "who is this person?").

At the time of writing, 54 countries are capturing some form of biometric data for voter registration.[20] Out of those, over two thirds rely on both fingerprint scans and photographs, combining fingerprint-matching with facial recognition technologies.

From a data protection and security point of view, the collection and storing of biometric data for voter registration raises significant concerns. Biometric data is particularly sensitive and revealing of individual's characteristics and identity, and as such it has the potential to be gravely abused.[21] As is increasingly recognised by data protection agencies around the world,[22] biometric data is often considered a special category of personal data attracting additional safeguards and limits for their collection and use. Further, identification systems relying on biometric data are also vulnerable to security breaches, whose consequences for the individuals concerned, and for the overall security of society are extremely grave.[23]

[18] With biometric voter registers, one or more physical characteristics of the voter, such as photo, fingerprint or retina scan, among others, are recorded at the time of registration. This information may be used for identification of the voter at the polling station.
[19] For a list of such concerns see the EU Handbook, https://www.eods.eu/library/EUEOM_Handbook_2016.pdf
[20] IDEA, ICTs in Elections Database – Voter registration and identification; question "If the EMB uses technology to collect voter registration data, is biometric data captured and used during registration?"; available at: https://www.idea.int/data-tools/data/icts-elections-database
[21] Report of the United Nations High Commissioner for Human Rights, 3 August 2018, A/HRC/39/29, available at: https://undocs.org/A/HRC/39/29
[22] ICO, Guidance on Biometric Data. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/guidance-on-biometric-data/key-data-protection-concepts/#special. AEPD, Use of Biometric Data: Assessment from a Data Protection Perspective. Available at: https://www.aepd.es/en/prensa-y-comunicacion/blog/biometric-data-assessment-from-a-data-protection-perspective
[23] See concerns related to the breaches of the Argentina ID database raised in the joint submission by Privacy International and Asociación por los Derechos Civiles in the context of Argentina's Universal Periodic Review, para.23. Available at: https://adc.org.ar/wp-content/uploads/2022/07/Adjunto-3-ADC-PI-UPR-Joint-Contribution.pdf

**Recommendations**

- Voter registration procedures should be clearly stipulated in law.
- The voters' register should not include personal data other than that which is required to establish eligibility to vote.
- The law should require the adoption of agreed international best practice on security to protect the voters' register against unauthorised access; it should also define the conditions and limits of access to the data contained in the voters' register.
- Personal data from the voter register should not be public by default. If there is to be an open register which anyone can buy access to for any purpose, this should operate on an opt-in as opposed to opt-out basis.
- It should be made clear in law and in relevant guidelines that personal data from the electoral register which have been made accessible are still subject to, and protected, by data protection law, including for onwards processing. In particular, personal data from the voter register should not be combined with other sources of personal data to create profiles of voters.
- Access to and use of personal data contained in a voter register should be regulated. Who is entitled to access and for what purposes should be clearly stipulated in the law, limited to what is necessary for the electoral process, with clear prohibitions on using this data for any other purpose.

Biometric voter registration

- Because of the special sensitivity of biometric data, its use requires robust safeguards enshrined in law, including recognition of this sensitivity in any data protection law.
- The law should stipulate that no third party other than the electoral management body should have access to the biometric data and that biometric data (including photographs) must not be used for anything other than deduplication and/or voter identity authentication.
- Additional protection for biometric data against unauthorised access or other data breaches should be developed, including storing biometric data separately from other data.
- Any open register to which access can be bought should not contain sensitive data, including biometric data.
- Robust privacy by design and by default needs to be applied to any systems related to voting. For example, systems should be designed for the specific use-case only and used only for authentication (1-1) rather than identification (1 to many).

**Questions**

- Does the law regulate the registration of voters and the administration of the voters' registry?
- What categories of data are included in the electoral register? (e.g. name, address, national ID number, ethnicity, etc.)
- Who is allowed to access the whole electoral register and what are the conditions for such access?
- Is a record kept of the entities having had access to part of or all of the electoral register, and if so, who is responsible for keeping such a record? Is this log regularly audited/proactively monitored for abnormal/unexpected access?

- What personal data is openly accessible, to whom, on what basis and under what conditions (e.g. consent of voter)?
- What security measures are adopted to ensure that the personal data contained in the voters' register is safe from unauthorised access? How often are these measures reviewed? And how are they assessed?
- Is the national data protection authority consulted on the administration and updates related to the voters' register?
- If biometric registration is used, is it subject to enhanced safeguards due to the special sensitivity of the data?
- If biometric registration is used, has it been designed with privacy in mind and limited to specific use cases of deduplication and/or voter identity authentication?

### 1.3. Voting

As noted by the UN Office of the High Commissioner for Human Rights, the way in which a country conducts voting operations and the degree to which they are transparent are crucial in ensuring the enjoyment of relevant human rights, in addition to increasing public trust in the process and the results.[24]

Voter verification is a key element of the voting operation. Similar considerations to the ones raised in relation to the voters' register apply, in particular about the need to limit collection of personal information of voters to what is strictly necessary in order to complete the process (see section 1.2 above). For instance, the data shared in the polling station should be limited to those necessary to identify the voter and complete the voting process. Further, States must take effective measures to ensure that all persons entitled to vote are able to exercise that right.[25] This obligation should include the removal of onerous obstacles to voter verification, such as requiring only one form of official ID to allow individuals to vote.[26]

As noted by the OHCHR, concerns have arisen with the digitalization of electoral processes and in particular electronic voting.[27] In line with this, the UN General Assembly has noted the 'use of online technology for balloting purposes' and reaffirmed the right to privacy in that context,[28] while the UN Secretary-General has recommended that the introduction of any new technology in the electoral context be tested prior to deployment, and for testing to consider the "increasing concerns regarding the vulnerability of national electoral infrastructures to cyberattacks".[29]

---

[24] OHCHR, Human Rights and Elections: A Handbook on International Human Rights Standards on Elections, 2021, para.125. Available at: https://www.ohchr.org/sites/default/files/2022-02/Human-Rights-and-Elections.pdf
[25] General Comment No.25, CCPR/C/21/Rev.1/Add.7, para. 11.
[26] See https://privacyinternational.org/news-analysis/4590/uk-government-should-drop-plans-compulsory-id-presentation-polling-station
[27] OHCHR, Human Rights and Elections: A Handbook on International Human Rights Standards on Elections, 2021, para.125. Available at: https://www.ohchr.org/sites/default/files/2022-02/Human-Rights-and-Elections.pdf
[28] UN General Assembly resolution on Strengthening the role of the United Nations in the promotion of democratization and enhancing periodic and genuine elections, U.N. Doc. A/RES/76/176, 11 January 2022.
[29] UN Secretary-General, Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization, U.N. Doc. A/74/285, 6 August 2019, para. 38. Available at: https://undocs.org/Home/Mobile?FinalSymbol=A%2F74%2F285&Language=E&DeviceType=Desktop&LangRequested=False

In recent years, researchers investigating e-voting initiatives have identified a range of challenges. In two separate analyses on e-voting initiatives deployed in the United States, MIT uncovered privacy issues as well as security vulnerabilities allowing for vote manipulation.[30] Similar flaws have been identified in connection with e-voting systems in Switzerland and Australia.[31]

**Recommendations**

- Avoid restricting the right to vote only to those in possession of national ID and provide for a wide range of ways to prove voters' identity to avoid discrimination and exclusion.
- Only the minimum personal data necessary to guarantee the integrity of the voting process should be required.
- Specific safeguards should be included to protect anonymity, minimise the risks of unauthorised access to data, and of hacking in the case of e-voting.
- Resources should be dedicated to election security, including establishing and conducting risk assessments for technologies used in elections.
- Mechanisms should be introduced to monitor, detect and warn against cyber-attacks on election infrastructure and integrated into the cyber security responses.
- Technical training and awareness of the cyber-security risks should be provided to those managing/involved on e-voting.

**Questions**

- How is voter verification primarily carried out? If voter verification relies on the presentation of an official identity document, are alternative documents/processes accepted in the absence of ID?
- Where voter verification is reliant on technology, are there alternative verification methods in case of failure of the machines?
- What personal data is demanded at the time of voting (i.e. for verification)?
- Of the personal data demanded at the time of the vote: (i) what is recorded, (ii) how is this recorded, stored and transferred, and (iii) to whom?
- What specific safeguards are in place to protect anonymity of voters in case of e-voting?
- If relying on electronic voting, electronic results transmission, or similar technologies, are there alternative ballot casting methods in case of power cuts/network failure/other equipment failures?
- What specific safeguards are in place to protect e-voting linked to the internet or other computer networks from unauthorised access and hacking?
- Is cyber security of elections included among the national cyber security strategy?
- What are the mechanisms available to monitor, detect and respond to cybersecurity attacks related to e-voting?
- Is training provided on cybersecurity for those involved in elections?

[30] Specter, Koppel and Weitzner, The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. Available at: https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf; Specter and Halderman, Security Analysis of the Democracy Live Online Voting System. Available at: https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot-1.pdf

[31] Jee, A major flaw has been found in Switzerland's online voting system, 12 March 2019. Available at: https://www.technologyreview.com/2019/03/12/136676/a-major-flaw-has-been-found-in-switzerlands-online-voting-system/ ; Halderman and Teague, The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. Available at: https://arxiv.org/abs/1504.05646

## 1.4. The role of the Election Management Body and other key entities in the electoral process

The Election Management Body (EMB) is the body (or bodies) responsible for ensuring impartiality, effectiveness, and transparency in elections.

Because of the prominent role of data and of digital technologies in the electoral process, it is imperative that EMBs have the technical expertise to assess how personal information and digital technologies processing such information are used in the electoral process. Otherwise, they risk jeopardising the integrity and security of the electoral register, which they typically manage. A 2022 audit of the Kenyan voter register found that access controls around the databases hosting the register of voters were ineffective, and that the proper authorisation procedures had not been consistently followed.[32]

Beyond developing their in-house expertise, there is continued recognition of the need for coordination among other government and independent regulatory bodies.[33] Threats to the integrity of elections come from different actors and require both the engagement of multiple authorities as well as coordination among them.

An ad hoc example of this kind of collaboration comes from the 2022 Kenyan election, where the Office of the Data Protection Commissioner, who received over 200 complaints from aggrieved individuals who were erroneously registered as members of political parties, worked alongside the Office of the Registrar of Political Parties to rectify the issue.[34] This collaboration can also be formally recognised. For example, the electoral management body in Mexico in its internal rules outlines an obligation for it to report to the data protection agency.[35]

Notwithstanding the above, instances of cooperation among authorities remain rare. For this reason, governments should consider setting up a coordinating mechanism, particularly in campaign and election periods, to ensure sharing of information and expertise among the different authorities with responsibilities in the running and monitoring of elections.

**Recommendations**

- EMBs should develop their expertise in data protection and cybersecurity.
- EMBs should cooperate with authorities in connected fields (such as data protection authorities, media regulators, cyber security authorities, biometric commissioners etc.) in a timely and effective manner.
- EMBs should regulate internal access to the voter register, and only selected staff members should have access to the voter register, subject to robust access controls and oversight mechanisms. To identify and address suspicious activity, EMBs should maintain a log of internal staff access to the voter register, and periodically review the log.

---

[32] See: https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert

[33] UNESCO, Elections in digital times: a guide for electoral practitioners, 2022, p.114. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000382102

[34] See: https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert

[35] See: Regulation of the National Electoral Institute on Personal Data Protection, Article 30. Available at: https://www.ine.mx/transparencia/protecciondp/marco-normativo/

- Where they exist independently from the EMB, regulatory bodies for political parties should encourage and facilitate compliance of political parties and candidates with data protection laws, including through connecting them to data protection agencies.

**Questions**

- Do EMBs have expertise in data protection and cybersecurity?
- What access controls are in place to ensure that access to the voter register by the staff members at the EMB is controlled, monitored, and limited to the role/function/task of the relevant individual seeking access?
- Does the EMB maintain a log of access to the voter register? If so, does it audit the log, with what frequency, and how effective is this audit?
- Is the EMB consulting and cooperating with other authorities (data protection, media regulators, cybersecurity)?
- Has the government set up a mechanism of coordination of authorities responsible for the various aspects related to the administration and monitoring of elections?

### 1.5.Private companies and procurement processes

Electoral processes are increasingly incorporating new technologies and digital processes, such as biometric voter registration and verification,[36] or the digital transmission of election results. These services are sometimes provided by private companies, who typically become involved in the conduct of elections following a tender process initiated by the relevant government setting out the relevant technical requirements for any product or service to be used in connection with the electoral process.

Generally, the privatisation of public tasks and responsibilities can be deeply problematic if deployed without the necessary safeguards.[37] The risks are exponentially higher in the electoral context, particularly where the use of technical products or services provided by a company are made essential to the voting exercise.

Once such technologies are adopted, they can generate dependency from governments, not least because they are costly to replace and/or private companies maintain control over the know-how to run and update those technologies. Contractual disputes can have tangible effects in the conduct of an electoral process, such as the postponement of an election or the withholding of nationwide databases.[38] Crucially, the design and functioning of a particular technology integrated into the electoral process can be called into question even after an

[36] As of late 2023, nearly 20% of countries worldwide use technology for identifying voters at polling stations. See IDEA, ICTs in Elections Database – Voter registration and identification; question "Is technology used for identifying voters at polling stations?". Available at: https://www.idea.int/data-tools/data/icts-elections-database
[37] Privacy International, Safeguards for Public-Private Partnerships, December 2021. See: https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships
[38] For election delays, Mali and Nigeria are recent examples - see https://www.aljazeera.com/news/2023/9/25/mali-postpones-february-presidential-election-due-to-technical-issues; and https://www.theguardian.com/world/2023/mar/09/nigeria-postpones-state-elections-dispute-presidential-vote. In Kenya, an election tech provider withheld a biometric database after unpaid instalments - https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert

election, and can be a key factor for judicial actors to consider in a legal action challenging the electoral outcome.[39]

It is essential that the relationship between a private company contracted for a specific product or technology to be used in the electoral process and an electoral management body is closely scrutinised from the earliest possible stage.

**Recommendations**

- EMB and private companies should ensure that robust human rights due diligence processes are in place, that include into their scope the early stages of the design and development of a technology, as well as stages of deployment and use.
- All documentation relating to the procurement process engaging a particular company for the provision of election technology should be made publicly available.
- Companies purporting to provide election technology should waive commercial confidentiality and make their technologies fully auditable to enable understanding of its functioning.
- Where personal data is envisaged to be processed by the relevant electoral technology, any provisional or final documentation should include details of prospective and actual data processing activities.
- Contracts for the provisioning of electoral technology should give explicit details of the company's access to data, and provide for corresponding safeguards to ensure security and proper handling of the data, especially when data is being sent internationally.

**Questions**

- What private company's technology does the administration of elections rely on? (e.g. biometric registration/verification kits)
- Is sufficient information made public about the procurement process and technology used to allow for public and regulatory scrutiny of the process and technology?
- What personal data does the private company providing technology have access to?
- What justification is provided for that data being processed?
- What safeguards or limits, if any, are imposed on the private company technology provider to processing data?
- Are there clear terms stating who retains ownership of the resultant dataset produced/maintained by a private company?

## 1.6.Complaints and redress

An independent complaints mechanism is necessary to ensure that electoral processes are free and fair and that all actors involved are accountable. In order for electors to have confidence in the electoral process, access to complaints or appeals processes and audit procedures should be provided by law.[40]

[39] In 2017, the Kenyan Supreme Court annulled the general election result based on range of factors, including the electoral management body's failure to conduct the transmission of election results in a credible manner. See full judgment here: http://kenyalaw.org/caselaw/cases/view/140716/

[40] OHCHR, Human Rights and Elections: A Handbook on International Human Rights Standards on Elections, 2021, para.128. Available at: https://www.ohchr.org/sites/default/files/2022-02/Human-Rights-and-Elections.pdf

Mechanisms of complaints and redress may well vary from country to country, but within the data protection framework there is a strong preference for the establishment of independent data protection authorities with the capacity to receive complaints coupled with the right of individuals for an effective judicial remedy against a decision of the data protection authority.[41] At the very least, these authorities should have the mandate to receive and investigate any complaints related to abuse of personal information in the electoral context. In 2021, following the receipt of fifty-one complaints, the Information Commissioner's Office in the UK fined the Conservative party for sending unlawful marketing emails in July 2019.[42] In 2022, the Office of the Data Protection Commissioner in Kenya received over two-hundred complaints about unsolicited text messages received by prospective voters erroneously identifying them as members of political parties.[43] More recently, the Brazilian Autoridade Nacional de Proteção de Dados imposed a fine on a small telecommunications firm, which the data protection agency investigated for offering bulk messaging services through WhatsApp to politicians.[44]

Additionally, data protection authorities should have the power to initiate investigations at their own discretion. In 2019, for example, the EDPS decided to run an investigation into the European Parliament's use of US-based political campaigning company NationBuilder to process personal data following ongoing concerns around the company, which resulted in the first-ever reprimands issued to an EU institution.[45]

Independent election regulatory authorities should also be empowered to receive complaints, particularly in relation to misuse of data by political parties and other political actors.

Similarly, individuals and organisations, including citizen observer groups, should be able to bring complaints for abuse of personal information in the election process to the national EMB or other national independent body monitoring the conduct of the elections.

**Recommendations**

- Independent data protection authorities should have the power to initiate investigations at their own discretion, as well as receive and act upon complaints by individuals and organisations denouncing abuse of personal data in the context of elections and political campaigns;
- Similarly, individuals and organisations should be empowered to bring complaints to EMBs or other independent election regulatory authorities;
- EMBs or other independent election regulatory authorities should have the authority to recommend and/or implement reforms when complaints reveal systemic problems;

[41] See, for example, Article 12 of Council of Europe Convention 108, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 and Article 77 of the EU General Data Protection Regulation.
[42] See https://ico.org.uk/media/action-weve-taken/mpns/2619896/conservative-party-mpn-20210601.pdf
[43] See https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert
[44] See https://www.dataguidance.com/news/brazil-anpd-imposes-fines-and-warning-telekall
[45] See the announcement by the European Data Protection Supervisor on the investigation into the European Parliament's 2019 election activities: https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigates-european-parliaments-2019_en; and their announcement closing the investigation: https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-closes-investigation-european-parliaments_en

- Individuals and organisations should also have the right to seek judicial remedies for alleged violations of data protection during elections, whether directly or by appealing the decisions of regulatory bodies.

**Questions**

- What mechanisms of redress are available to individuals and organisations complaining about abuses of personal data in the context of elections and political campaigns?
- Does the EMB accept complaints by individuals and organisations?
- What are the remedies available (fines, imposition of conditions or restrictions in the processing of personal data, etc.)?
- Is it possible for the DPA to initiate investigations on their own initiative?

## Part 2 - Political parties and other political actors

There is growing recognition by election monitoring organisations that the rules regulating the conduct of political parties and other actors during elections need to be assessed in light of the increased reliance on technologies and on personal data.

As recognised by the Council of Europe in its 2021 issued guidelines, with elections having become increasingly "data-driven", it is critically important that all organisations involved in political campaigns process personal data on voters in compliance with well-established data protection principles.[46]

### 2.1.Regulation of the use of personal information by political parties

Political parties and other political actors are increasingly employing a wide array of data-intensive techniques to target potential voters. These techniques rely on the collection and analysis of personal information. Personal information is understood as a political asset, which can be used to effectively target groups in order to encourage their support or hinder their participation in political processes, based on individual or shared characteristics.[47]

Personal data revealing political opinions is a special category of data under modern data protection laws, the processing of which is subject to strict safeguards and generally prohibited with narrowly-interpreted exceptions, such as the explicit, specific, fully-informed and freely-given consent of the individuals affected.[48] The Council of Europe has noted that the processing of such data entails severe risks of voter discrimination – leading to voter suppression and intimidation – and may potentially affect the provision of government services.[49] For these

[46] Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, November 2021, p.5. Available at: https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72

[47] An investigation by Channel 4 found that a campaign strategy deployed by Donal Trump in the 2016 election aimed to deter millions of African-Americans from voting. See: https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

[48] Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, November 2021, paras. 4.2.1 – 4.2.4. Available at: https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72

[49] CoE, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, November 2021, para. 4.2.4. Available at: https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72

reasons, the processing of special categories of data needs to be accompanied by safeguards appropriate to the risks at stake.[50]

Increasingly, however, political opinions can be revealed or inferred through predictive analytical and profiling tools from a range of sources of information, including those that may be public, such as magazines and newspapers read and membership in interest groups, among others.[51] In light of the growth of technologies allowing for such inferences to be made, some regulators and oversight bodies have narrowed the scope for such processing to take place. For example, the Spanish data protection authority expressly prohibited the processing of personal data from which political opinions could be inferred based on the application of technologies such as artificial intelligence.[52]

Despite these risks, data protection laws can include exemptions to data protection requirements for political parties.[53] These exemptions risk undermining efforts to address the exploitation of personal data during elections.

Data protection regulators are increasingly taking steps to investigate the use of voters' data by political parties. In 2020, the ICO undertook an audit of the use of personal data by political parties following previously articulated concerns about the use of personal data in political campaigning.[54] In 2021, the Irish Data Protection Commission audited the practices of political parties in Ireland in response to public concerns around a party's storage of the information of millions of voters on an internal database.[55]

**Recommendations**

- Data protection laws should be fully applied to the processing of personal data by political parties and other political actors;
- Political parties and other political actors should:
    - be transparent about their data processing activities, including identifying the mechanisms they use to engage with voters (e.g. social media, websites, direct messaging and campaign and targeting methods) and what personal data they process;
    - be transparent about how they collect people's data and the sources of this;
    - be transparent as to their profiling practices, including any practices of their processors or joint controllers, including making inferences, as well as explaining any automated decision-making;
    - be transparent on their political ads and messaging, ensuring that the public can easily recognise political messages and communications and the organisation

[50] Ibid.
[51] Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, November 2021, para. 4.22. Available at: https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72
[52] AEPD, https://www.boe.es/buscar/doc.php?id=BOE-A-2019-3423
[53] See: https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation-political-parties
[54] ICO, UK Political Parties, 11 November 2020. Available at: https://ico.org.uk/action-weve-taken/audits-and-overview-reports/uk-political-parties/
[55] Irish Data Protection Commission, Data Protection Audit of Political Parties in Ireland, December 2021. Available at: https://www.dataprotection.ie/en/news-media/latest-news/data-protection-commission-publishes-report-data-protection-audit-political-parties-ireland

behind them. They should make available information on any targeting criteria used in the dissemination of such political messages;
- publish a complete, easily accessible and easily understandable list of any campaign groups they have financial or informal collaborative campaigning relationships with, including all third parties and joint campaigners;
- be transparent as to the companies they contract with as part of their campaigns both to obtain data and to further process data, including profiling and targeting, such as data brokers and political advertising companies, as well as which companies are providing campaign tools/software and the products they are using;
- adopt and publish data protection policies;
- carry out data protection audits and impact assessments;
- ensure they have a legal basis for each use of personal data (including any sensitive data such as that reflecting political opinions);
- before using personal data provided by any third party, ensure that the data has been obtained lawfully and that the third party is in compliance with data protection laws;
- facilitate the exercise of data rights by individuals (including providing information about how their data is processed, and providing access and allowing for its updating and erasure), and publish mechanisms and procedures for reporting and responding to concerns; and
- take appropriate security measures to ensure against unauthorized access to, or disclosure of personal data. These measures should take into consideration the communications and technologies used, and include: training in privacy and security; access controls; confidentiality agreements; and controls on physical access to places and equipment where personal data are stored.

**Questions**

- Does the national law on data protection apply to the data collected and used (processed) by political parties and other political actors?
- Do political parties and other political actors have data protection policies?
- Do those policies provide clear, accessible and understandable information about how to exercise data rights?
- Do they disclose where the political parties and other political actors get the personal data and what they do with it?
- Do the political parties and other political actors carry out data protection impact assessments relating to their processing of personal data?
- Have they obtained consent for the individuals or how else do they justify holding the data?
- Do political parties and other political actors assess the data protection compliance of any third parties they are using for their campaign activities and whether they are acting lawfully?
- What security measures do they take to prevent unauthorised access to or sharing of personal data?
- Do they train all those involved in their political campaigns on privacy and data security measures?

## 2.2.Regulation of data-driven political campaigns

Political campaigns around the world have turned into sophisticated data operations, with individuals' personal data increasingly used to target them with personalised advertising.

Since the Cambridge Analytica scandal,[56] examples of political campaigning relying on personal data have continued to emerge. Human Rights Watch reported that the 2022 Hungarian elections were characterised by data-driven campaigning, with evidence suggesting that the ruling party repurposed data collected by the state for administering public services to spread its own campaign messages.[57]

Micro-targeting and other data-driven targeting techniques used by the broader digital advertising industry are increasingly deployed in the political campaigning context.[58] Various companies, known as data brokers, sell data to political campaigns that can be used to better target voters. An investigation by the Markup revealed that the data points offered by data brokers ranged from voters' likely views on abortion or gun control, to the location data of individual voters.[59]

Some of the risks identified in connection with mass profiling and micro-targeting include the creation of filter bubbles or echo chambers, voter discrimination, disenfranchisement, the possible chilling of political participation, increased polarisation, the erosion of robust democratic debate, and the weakening of election integrity.[60]

The risks around the use of personal data for political advertising have prompted extraordinary condemnation, as well as regulatory efforts. The UN and OAS special rapporteurs on freedom of expression have called for political advertising targeted at individuals based on personal data to be disallowed in the absence of the individuals' consent to the use of their personal data for this purpose.[61] At the time of writing, the European Union's draft Regulation on transparency and targeting of political advertising is in its final legislative stages, with lawmakers still undecided as to whether the use of special categories of data should be allowed for online

---

[56] Cambridge Analytica was a company that operated as a UK based political consultancy. One of the key services it offered was a unique 'psychographic' profile of voters. It was used in a number of US campaigns and possibly the Leave.EU campaign in the UK. See, among many, European Parliament Resolution on the Use of Facebook Users' Data by Cambridge Analytica and the Impact on Data Protection, 2018/2855(RSP), 25 October 2018.

[57] Human Rights Watch, Trapped in a Web – The Exploitation of Personal Data in Hungary's 2022 Elections, December 2022. Available at: https://www.hrw.org/report/2022/12/01/trapped-web/exploitation-personal-data-hungarys-2022-elections

[58] As Alexander Nix CEO of Cambridge Analytica is reported as having said "What we are doing is no different from what the advertising industry at large is doing across the commercial space". Witness I: Alexander Nix, Chief Executive, Cambridge Analytica, Digital, Culture, Media and Sport Committee Oral Evidence: Fake News (HC 363), 27 February 2018. available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media- and-sport-committee/disinformation-and-fake-news/oral/79388.pdf (last visited 30 October 2023).

[59] The Markup, How Political Campaigns Use Your Phone's Location to Target You, 8 November 2022. Available at: https://themarkup.org/privacy/2022/11/08/how-political-campaigns-use-your-phones-location-to-target-you

[60] Council of Europe, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, November 2021, para. 2.10.

[61] UN, OAS and OSCE, Joint Declaration on Freedom of Expression and Elections in the Digital Age, April 2020. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclarationDigitalAge_30April2020_EN.pdf

political ads.[62] Other laws, such as the EU Digital Services Act, have outrightly prohibited advertisements based on profiling using special categories of personal data.[63]

A few of the key practices that continue to gain prominence and are increasingly deployed in the political campaigning context are outlined below.

- Profiling

Profiling refers to "any form of automated processing of personal data, including use of machine learning systems, consisting in the use of data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[64] Personal data – whether provided, automatically collected, derived, inferred, or predicted – is used to develop detailed profiles of both individuals and groups. The data that feeds into such profiles is bought, amassed and shared from and between multiple actors[65] often without individuals having ever known that they were profiled. Profiles can be cross-correlated and used to infer data not just about an individual but others 'like them', for example through 'lookalike audiences'.[66] Furthermore, data brokers and ad tech companies often offer probabilistic solutions, where they will establish "a match between sets of data leveraging inferred, modelled or proxy assumptions".[67]

- Data-driven techniques

*Micro-targeting*

The practice of micro-targeting is better understood as a four-step process relying on (i) data collection; (ii) profiling, by dividing individuals into small groups or "segments" based on real or perceived characteristics, interests or preferences; (iii) the personalisation of content based on such characteristics; and (iv) targeting and delivering this content, often through online platforms.[68] By its very nature, micro-targeting is likely to involve a multiplicity of actors, ranging from data brokers supplying personal data, to the political campaigns developing the messaging, and online platforms facilitating the delivery of messages. An example of the complementary role that social media platforms can play in the delivery of micro-targeting is

[62] See https://edri.org/our-work/political-negotiations-continue-eu-lawmakers-fail-to-agree-on-strong-rules-for-regulating-political-advertising/
[63] See Digital Services Act, recital 69; Article 26(3).
[64] Council of Europe, Recommendation CM/Rec(2021)8 of the Committee of Ministers to members States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 3 November 2021, para 1(c).
[65] Privacy International, Our Complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad, 8 November 2018, available at https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad
[66] Information Commissioner's Office, Democracy Disrupted? Personal Information and Political Influence, 11 July 2018, p. 36. Available at: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf
[67] Winterberry Group, "Know Your Audience: The Evolution of Identity in a Consumer-Centric Marketplace", August 2018. Available at: https://marketing.acxiom.com/US-Parent-Winterberry-KnowYourAudience-REP-Main.html?&utm_source=website&utm_medium=owned&utm_campaign=identityresolution
[68] See https://privacyinternational.org/learn/micro-targeting

the use of ad-targeting categories which may act as proxy data for specific characteristics such as "pseudoscience" or "conspiracy theory".[69]

Micro-targeting remains largely unregulated despite related concerns. A 2021 research paper from the University of Edinburgh exploring the regulatory landscape for political campaigning across six countries found that not a single country defined or comprehensively regulated micro-targeting.[70] Nevertheless, regulatory bodies are pressing for robust regulation. In its opinion on the proposed EU regulation on political advertising, the European Data Protection Supervisor called for a full ban on micro-targeting for political purposes.[71]

*Geo-fencing*
Geo-fencing makes it possible for individuals to be dynamically targeted on the basis of their location. This practice can reveal sensitive data and present significant risks to individuals.[72] For example, has been reported that religious groups have used such technology to target individuals attending religious locations.[73]

***
It is important to recognise that the above targeting techniques (whether by political parties or other political actors) are deployed not only during the campaign election period. The misuse of personal data for manipulation and disinformation, as seen during and in the aftermath of the Covid-19 pandemic, is an ongoing phenomenon that has been the subject of a range of reports and resolutions by UN human rights bodies, including a UN Human Rights Council Resolution.[74] In Privacy International's view, and in keeping with the continuous nature of information-sharing and data collection, the regulation of the use of data for political campaigning should not be time limited to the election period.

There is a plethora of companies and other actors, beyond political parties and candidates, that use (or offer) these data-intensive and privacy-invasive targeting techniques. Focusing only on the campaign election phase and on the political parties or official candidates risks missing a significant part of the picture.

**Recommendations**

- Laws and regulations should require the disclosure of information on any targeting criteria used by political parties and others in the dissemination of political communications.

[69] Both of these ad-targeting categories were used by Facebook and subsequently removed. See: https://www.reuters.com/article/us-health-coronavirus-facebook-ads-idUSKCN2253CC
[70] See Privacy International and University of Edinburgh, Micro-targeting in political campaigns: a comparative analysis of legal frameworks, January 2021. Available at: https://privacyinternational.org/report/4364/micro-targeting-political-campaigns-comparative-analysis-legal-frameworks
[71] European Data Protection Supervisor, EDPS Opinion on the Proposal for Regulation on the Transparency and Targeting of Political Advertising, 20 January 2022, paras. 26-34. Available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-regulation-transparency-and_en
[72] Council of Europe, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, November 2021,
[73] See https://www.npr.org/2020/02/06/803508851/how-political-campaigns-are-using-geofencing-technology-to-target-catholics-at-m
[74] See UN Human Rights Council Resolution A/HRC/RES/49/21. Available at: https://digitallibrary.un.org/record/3971994

- In case of data-driven targeting techniques, adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it, and how they can exercise their rights to protect their data and prevent being targeted.
- Political parties and other political actors should ensure that the public can easily recognise political messages and communications and the party, foundation or organisation behind them. They should make available on their websites and as part of the communication, information on any targeting criteria used in the dissemination of such communications.
- No personal data shall be shared by political parties and other political actors with social media companies for the purposes of digital advertising without appropriate notification to the data subjects.
- Political parties and other political actors must ensure that the use of data in such techniques (by them and those that they work with to get data) complies with all the requirements of data protection law, including principles such as transparency, fairness and purpose limitation, the requirement to have a legal basis, rights such as the right to information and erasure and obligations such as conducting a data protection impact assessment.
- Political campaigns should be transparent as to the third parties they contract with as part of their campaigns both to obtain data and to further process data, including profiling and targeting, such as data brokers and political advertising companies.

**Questions**

- Do laws or regulations require political parties and other actors to disclose links to organisations/individuals associated with them which carry out political advertising or campaigning, including online?
- Do laws or regulations require political parties or other actors, to provide information to individuals and to regulators about their use of targeting techniques, including the targeting criteria, and which third parties they are working with?
- Does the current regulatory framework make it possible for the public or the regulator to identify the full range of third parties involved with the political party? (e.g. does it cover subcontractors?)
- Do political parties and other political actors take sufficient responsibility over the data that any third parties with which they contract may use? Do they know what data those third parties are using? What contracts do they have with the third parties? Do those contracts contain sufficient data protection and security clauses?

### 2.3.Campaign financing

Campaign finance refers to both the funding provided to political parties or candidates for the purpose of the election campaign (either through private donations or public funding) and the spending by the parties or candidates on campaign expenses.

Political parties and other actors are increasingly using social media platforms and other digital communications means both for targeting potential individual donors (particularly for small donations) and for spending on political advertisement.

Campaign financing is notoriously difficult to monitor. Research carried out in Colombia by Dejusticia found that the online monitoring tool operated by the National Electoral Council to provide information about campaign spending failed to guarantee transparency regarding the

contracting of digital marketing and political communication services.[75] A recent study carried out in the UK found that nearly 15 per cent of spending by political parties during the 2019 UK general election campaign is unaccounted for, while £10 million had been spent on advertising, 73 percent of which had been online; and that current expenditure categories for political campaigns did not reflect the reality of modern campaigning.[76]

As noted by the European Data Protection Supervisor's in its 2018 report on online manipulation and personal data, the reported spending on campaign materials still fails to provide sufficient details about spending on digital advertising and associated services.[77]

**Recommendations**

- Campaign finance laws should require timely reporting on spending on online campaigning and on the funding obtained online. The information should be sufficiently granular and detailed to promote transparency and accountability.
- Laws and regulations should require the public disclosure of campaign spending by candidates and political parties in connection with obtaining and processing personal data, in particular contracts with third parties such as data brokers and political advertising companies.
- Political parties and other political actors should make publicly available (e.g. prominently on their websites) information on their expenditure for online activities, including paid online political advertisements and communications. This should include information regarding which third parties, if any, have directly or indirectly assisted the political actors with their online activities, including the amount spent on each third parties' services.
- Disclosure of campaign expenditure should be broken down into meaningful categories such as amount spent on types of content on each social media platform, information about the campaign's intended target audience on platforms, as well as actual reached audience.
- National laws and regulations (e.g. code of practice) should require the disclosure of information on groups that support political campaigns, yet are not officially associated with the campaign, and disclosure of campaign expenditure for online activities, including paid online political advertisements and communications.

**Questions**

- Do campaign finance laws require reporting on spending on online campaigning? To whom? How granular are those requirements? Within which timescale? What are the sanctions for failing to comply?
- Do laws or regulations require political parties (and other political actors) to disclose the amount paid for online political advertisements? What are the details of such disclosure (e.g. disaggregated by digital platforms; etc.)?

---

[75] Dejusticia, Digital Technologies and Political Campaigns: A Risk for the 2022 Elections?, 30 November 2021. Available at: https://www.dejusticia.org/en/digital-technologies-and-political-campaigns-a-risk-for-the-2022-elections/

[76] IDEA, Regulating the Business of Election Campaigns, 20 May 2022. Available at: https://www.idea.int/publications/catalogue/regulating-business-election-campaigns

[77] European Data Protection Supervisor, Opinion 3/2018 on online manipulation and personal data, 19 March 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

- Are political parties and political actors disclosing their online campaigning expenditures with sufficient granularity?

## Part 3 - Role of internet and social media in election and political campaigns

The Internet and social media have helped many to organise politically, to participate in public debates, to express opinions (including dissent) online, and to receive information, including during election campaigns.

At the same time, current digital communications technologies have put into question the effectiveness of some of the safeguards adopted to ensure free and fair elections. Particular attention has been paid to the spread of disinformation and the risk of manipulation of individuals' political opinions. Most of the analysis and policy or regulatory developments in this area have focussed on the content of digital communications, including efforts to moderate or take down content, especially by internet and social media companies. Relatively less attention has been paid to the personal data collected and processed to allow such content to reach desired audiences, despite the concerns that the exploitation of personal data negatively affects voters. These concerns are heightened closer to election periods, but they are relevant anytime given how even seemingly non-political online content can result in the mobilisation of people politically.

### 3.1.The 'scarcity' assumption

A key campaigning safeguard is to ensure that political parties and other contestants have equal and fair access to traditional media and that reporting by publicly owned media is fair and not partisan.

The rationale for these obligations (of impartiality, fairness, balance, and equality during elections) is the 'scarcity assumption', i.e. the fact that opportunities to access traditional media are limited. This 'scarcity', it has been traditionally assumed, would not apply to online media, given the facility and variety of sources of opinions and free access to them.

However, this assumption does not take into consideration the market concentration and business models in the digital communications field and the way information is distributed and shared by digital platforms (notably search engines and social media platforms, including messaging apps.)[78]

In particular, search engines and social media platforms filter the news and opinions users can access based on profiling, which is usually highly dependent on data exploitation. This goes beyond paid-for targeted advertisements and promotion of content to the way all content is displayed and recommended.[79] Reflecting on the challenges posed by the prevailing digital communications landscape, the UN Special Rapporteur on freedom of expression noted that "by designing their products with highly personalized content to encourage addictive

[78] One example is Google paying $26.3 billion to be the default search engine everywhere, which overwhelmingly exposes consumers to Google's search results, as opposed to other search engines'. See: https://www.theverge.com/2023/10/27/23934961/google-antitrust-trial-defaults-search-deal-26-3-billion

[79] For example, the personalisation of Google search results https://www.google.com/search/howsearchworks/algorithms/; Facebook's newsfeed https://www.facebook.com/help/1155510281178725 or YouTube's recommendations https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

engagement, companies further promote a system that significantly undermines people's agency and choice in relation to their information diet."[80]

These data targeting techniques expose individuals only to selected political messages and political information, directly challenging the assumption that a wide spectrum of opinions and content in the online media is easily available to anyone. Effects like filter bubbles, etc. are direct consequences of profiling and have significant effects on the formation of political opinions and ultimately on elections. As recommended by the UN Special Rapporteur, "companies should provide clear and meaningful information about the parameters of their algorithms or recommender systems and ensure that those systems enable users to receive a diversity of viewpoints by default while also enabling them to choose the variables that shape their online experience."[81]

**Recommendations**

- Internet and social media platforms must be transparent about their profiling activities, including for the personalisation of what people see.
- Companies should provide clear and meaningful information about the parameters of their algorithms or recommender systems and ensure that those systems enable users to receive a diversity of viewpoints by default while also enabling them to choose the variables that shape their online experience.
- The use of personal data for profiling including the personalisation of content must comply with data protection standards.

**Questions**

- Have social media platforms made any specific commitments or introduced any measures related to the display of content in upcoming elections, such as ad transparency?
- What are the ways in which political actors can reach users on their platform? How do their advertising, profiling, targeting and recommendation services work? Who can access those services?
- Do the platforms comply with national data protection legislation?
- Do the major platforms have an in-country contact person? What mechanism is available for reporting abuse and addressing complaints?
- Are there any laws or regulations which enable electoral management bodies to request specific user information from social media platforms?

### 3.2.Transparency of political ads and issue-based ads

A key feature of modern political advertising is that political parties and other actors can target voters using multiple sources of data and/or mechanisms, some of which are provided by third parties such as social media platforms or data brokers. In its 2020 guidelines, the European Data Protection Board (comprising the Data Protection Authorities of the 27 EU member states) recognised the multiplicity of actors and sources of data involved, noting that the criteria used to target individuals "may have been developed on the basis of personal data which users

[80] Report of the UN Special Rapporteur on freedom of expression, para 66, U.N. Doc. A/HRC/47/2.
[81] Report of the UN Special Rapporteur on freedom of expression, para 99, U.N. Doc. A/HRC/47/2.

have actively provided or shared, […] on the basis of personal data which has been observed or inferred, either by the social media provider or by third parties, and collected (aggregated) by the platform or by other actors (e.g., data brokers) to support ad-targeting options."[82]

In its Guidelines, the Council of Europe has emphasised the need for political campaign organisations to provide voters with "adequate information on why they are seeing a particular message, who is responsible for it, and how they can exercise their rights to prevent being targeted; and information on any targeting criteria used in the dissemination of such communications […] the voter should have the right to know "why I am seeing this ad."[83]

Recent legislative developments in the European Union have imposed additional obligations to enforce transparency in political advertising. Building on the requirements imposed by the recent EU Digital Services Act,[84] the draft regulation on political advertising expands the categories of information to be disclosed in the context of political advertising where advertisers use targeting or amplification techniques. Such information includes the specific groups of recipients targeted, including the parameters used to determine the recipients to whom the advertising is disseminated, the categories of personal data used for the targeting and amplification; where applicable, information that the personal data was derived, inferred, or obtained from a third party and its identity as well as a link to the data protection notice of that third party for the processing at stake; as well as a link to an effective means to support individuals' exercise of their data protection rights.[85]

While the reach and effectiveness of these efforts to improve transparency remain to be seen, there is an increased recognition that transparency on political advertising can benefit civil society, researchers, and election observers as they conduct assessments of online engagement prior and during elections.

**Recommendations**

- National laws and regulations (e.g. code of practice) should require companies to be transparent regarding paid online political advertisements and communications, including by providing users with adequate information on why they are seeing a particular message, who is responsible for it, and how they can exercise their rights to prevent being targeted.
- Internet platforms, including search engines and social media platforms, should publicly disclose all advertising including political advertising and political issue-based advertising. Disclosure should at least include targeting parameters (intended audience, actual audience, profiles) and who paid for the ads.

---

[82] European Data Protection Board, Guidelines 8/2020 on targeting of social media users, 2 September 2020. Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf

[83] Council of Europe, Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns, November 2021, para. 4.4.5.

[84] The DSA imposes obligations on selected online platforms - Very Large Online Platforms ("VLOPs") and Very Large Online Search Engines ("VLOSEs") - to create repositories of advertisements presented on their online interfaces, including information as to who paid for the ad and/or its delivery, data on the advertiser, as well as targeting criteria and delivery criteria. See Recital 95 and Article 39.

[85] Draft Regulation on the transparency and targeting of political advertising, Article 12 and Annex II.

- The platforms should establish political ads libraries providing privacy-compliant access for researchers to track and better understand the spread and impact of these political advertisements and the targeting deployed.

**Questions**

- How is online political advertising and issue-based advertising defined and regulated in law?
- Have the main Internet platforms operating in the country developed policies for transparency of political ads and other political communications, and of targeting?
- Have the main Internet platforms operating in the country enabled access for public interest researchers and relevant regulators to monitor and review the ads in the run up to the election?

## Conclusion

There is growing recognition at international level of the myriad ways in which personal data is used in connection with electoral processes, as well as the risks that some data processing poses to the integrity, fairness and freedom of elections.

Election observer organisations are uniquely positioned, by virtue of their knowledge and understanding of the relevant local context – and as the case may be, of international electoral practice – to digest and comment on the technology and data dimensions of any electoral process at issue.

For this reason, election observer organisations have a fundamental role to play to ensure digital technologies are employed in ways that protect and promote the rights of voters and ultimately support free and fair elections. To perform their role effectively, they need to review and update their election observer methodologies so that they are able to detect concerns related to the use of data and digital technologies and to provide remedial recommendations.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org