TECHNOLOGY, DATA & ELECTIONS: A Checklist on the Election Cycle

June 2019

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).

Technology, Data and Elections: A Checklist on the Election Cycle

June 2019

Introduction

Democratic engagement is increasingly mediated by digital technology. Whether through the use of social media platforms for political campaigning, biometric registration of voters and e-voting, police monitoring of political rallies and demonstrations using facial recognition, and other surveillance methods, technology is now infused into the political process.

As noted in the EU third edition of the Handbook for European Union Election Observation:

"The rapid development of information and communication technologies (ICTs) has also had a significant impact on the conduct of elections, offering new promises and challenges for election administrators, voters and observers alike. ICTs are reshaping not only the conduct of crucial aspects of the election processes such as voter registration and balloting procedures, but also the whole democratic environment, with web-based media allowing new opportunities of exchanges of opinions and information between people."[1]

These technologies rely on collecting, storing, and analysing personal information to operate.[2] Much recent debate around elections has focussed on the content of digital communications, e.g. 'fake news' and disinformation. But the hidden data exploitation system on which many of these technologies rely also poses significant threats to free and fair elections.

In democratic elections, political parties and campaigners use these technologies – that rely on personal information – to reach out to potential voters. Also, electoral management bodies (EMBs) across the world are increasingly relying on biometric data registration.

Further the reliance on digital technologies for all aspects of election campaigns and election processes increases elections' vulnerability to cyber-attacks. The most significant consequence of such digitalisation is that measures to protect against cyber-attacks need to be considered for the whole election campaign and processes, from the setting of the electoral registry to e-voting, from the databases of voters and supporters managed by political parties to the data collected and used by other actors, such as social media platforms, data brokers and the ad tech industry.[3]

[1] See: https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf
[2] See: https://privacyinternational.org/topics/data-and-elections
[3] See Stiftung Neue Verantwortung, Securing Democracy in Cyberspace - An Approach to Protecting Data-Driven Elections, October 2018, https://www.stiftung-nv.de/sites/default/files/securing_democracy_in_cyberspace.pdf

In this context, international election observers are increasingly called upon to consider the role of personal data and the digital technologies that are used by all main actors in democratic elections. This is not an easy task. It will require updating existing election observers' methodologies and acquiring new technical skills.

Notwithstanding these challenges, Privacy International believes that international election observers are well placed to address them and can play a significant role in ensuring that personal data and digital technology are used to support, rather than undermine, participation in the democratic process and the conduct of free and fair elections.

In the following sections, Privacy International identifies the main areas where technology and the processing of personal data play a key role in the electoral process. The briefing is organised to follow the methodologies developed by election observer organisations.[4] 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.

The first part covers the overarching legal framework and the relevant regulations related to the administration of elections (voter registration, voting, and the role of the Electoral Management Body.) 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 private companies, notably search engines and social media platforms, in the context of elections (with particular focus on transparency of political advertising.)

[4] See Promoting Legal Frameworks for Democratic Elections (https://www.ndi.org/sites/default/files/2404_ww_elect_legalframeworks_093008.pdf); EU third edition of the Handbook for European Union Election Observation (https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf); OSCE/ODIHR election observation handbook (6th edition, https://www.osce.org/odihr/elections/68439?download=true)

Part 1 – Administration of elections

1.1 Legal framework – protection of the right to privacy

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.

The protection of personal information is inextricably linked to the right to privacy.[5] As noted by the European Commission, data protection is necessary for democratic resilience[6] and data protection law provides some of the tools necessary to address instances of unlawful use of personal data in the electoral context.

Reflecting the fundamental right to privacy embodied in international law, 134 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 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.[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.

[5] For example, according to the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, "the right to privacy" includes "the ability of individuals to determine who holds information about them and how ... that information [is] used." U.N. Doc. A/HRC/23/40, para 22, 17 April 2013. See also UN High Commissioner for Human Rights report on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29, 3 August 2018.
[6] See: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf
[7] As of April 2019, see https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386510.
[8] Privacy International has developed a guide on data protection legislation, which identifies relevant international and regional standards and best practices: https://privacyinternational.org/data-protection-guide
[9] See: https://privacyinternational.org/news-analysis/2836/gdpr-loopholes-facilitate-data-exploitation-political-parties

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".[10] Some of the data intensive techniques deployed in the context of elections and political campaigning (profiling, microtargeting, etc. detailed in section 2.2 below) can constitute manipulative unlawful interference with the right to form opinions and to be informed.

Recommendations:

- National laws, ideally the Constitution, should recognise the right to privacy (including of data protection);
- A modern, comprehensive data protection law should be in place with an independent, sufficiently resourced data protection authority. It 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.[11]
- 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, including political campaigns.

[10] See Human Rights Committee, General Comment 25.
[11] For more information on what a comprehensive data protection law should include, see: https://privacyinternational.org/report/2255/data-protection-guide-complete

Questions:

- Does the constitution or other legislation protect the right to privacy and data protection?
- 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?
    - 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 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. 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 and political organisations) is necessary to safeguard the fairness of the electoral process, 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' register 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, 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 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. There are concerns that this database has been 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. It is not clear who the registration database was shared with and therefore which company, if any, was responsible for this microtargeting. Privacy International's partner, the Centre for Intellectual Property and Technology Law (CPIT) at Strathmore University, Kenya, researched whether the 2017 voter register was shared with third parties, and if so, with whom, finding more questions than answers.[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.

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[14], for

[12] See: https://sur.conectas.org/en/a-very-secret-ballot/
[13] https://privacyinternational.org/report/2066/investigating-privacy-implications-biometric-voter-registration-kenyas-2017-election
[14] See: https://ico.org.uk/your-data-matters/electoral-register/

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 is often used for marketing purposes. Therefore, an entity with access to the full registry 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.

In March 2016, the personal data of over 55 million registered Filipino voters were leaked following a breach on the Commission on Elections' (COMELEC's) database.[15] The investigation of the national data protection authority concluded that there was a security breach that provided access to the COMELEC database that contained both personal and sensitive data, and other information such as passport information and tax identification numbers. The report identified the lack of a clear data governance policy, vulnerabilities in the website, and failure to monitor regularly for security breaches as main causes of the breach.

- **Biometric Voter Registration (BVR)[16]**

Proponents of BVR argue that it is effective against voter frauds, 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's dependency.)[17]

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 the purpose of

[15] https://www.privacyinternational.org/state-privacy/1009/state-privacy-philippines
[16] 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.
[17] For a list of such concerns see the EU Handbook, https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf

deduplicating is that the result 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?").

From a data protection and security point of view, the collection and storing of biometric data for voter registration raises additional concerns. Biometric data is particularly sensitive and revealing of individual's characteristics and identity. As such it has the potential to be gravely abused.[18] Under many data protection laws, biometric data is 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.[19]

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 define the minimum standards of 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.

[18] 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

[19] For examples of breaches of biometric databases, see Privacy International, Briefing to the UN Counter-Terrorism Executive Directorate on the responsible use and sharing of biometric data in counter- terrorism, June 2019.

- Access to and use of personal data contained in an electoral 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.
- Biometric data (including photographs) must not be used for anything other than the stated purpose in law (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.
- No third party (other than the public authority which manages the voter registration process) should have access to the biometric data.
- Transparency in contracts with suppliers, and safeguards surrounding data being sent internationally.
- Robust privacy by design and by default needs to be applied. 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?
- Who is allowed to access the whole electoral register and what are the conditions for such 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, relevant use cases?

1.3 Voting

Rules around voting aim "to ensure that all eligible voters have a genuine opportunity to freely cast a secret ballot, illegal voting is prevented, the will of the voters is registered, fraud is prevented, and transparency provides a basis for public confidence in the electoral process."[20]

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, increased reliance on technical solutions, such as e-voting, raise additional risks of abuse and specific challenges related to cybersecurity and the protection of anonymity of voters. These concerns have been articulated by some election observers' organisations, noting, for example, that "e-voting systems linked to the Internet or other computer networks may be susceptible to hacking or outside manipulation."[21] In a comprehensive report, Security Democracy in Cyberspace, the German organisation Stiftung Neue Verantwortung details a range of measures related to cybersecurity and elections.[22] Some of the relevant recommendations contained in that report are reflected below. Further, in the

[20] See Promoting Legal Frameworks for Democratic Elections (https://www.ndi.org/sites/default/files/2404_ww_elect_legalframeworks_093008.pdf)
[21] See EU third edition of the Handbook for European Union Election Observation (https://eeas.europa.eu/sites/eeas/files/handbook_for_eu_eom_2016.pdf)
[22] See Stiftung Neue Verantwortung, Securing Democracy in Cyberspace - An Approach to Protecting Data-Driven Elections, October 2018, https://www.stiftung-nv.de/sites/default/files/securing_democracy_in_cyberspace.pdf

US context, the Center for Democracy & Technology developed useful guides to raise awareness of the security risks surrounding the use of e-voting technologies.[23]

In practice, even countries with significant experience in organising elections and referenda are susceptible to these risks. For example, in Switzerland researchers found technical flaws in the electronic voting system that could enable outsiders to replace legitimate votes with fraudulent ones.[24]

Recommendations:

- 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:

- What personal data is demanded at the time of voting (i.e. for verification)?
- What personal data is stored, how is it transferred and to whom?
- What specific safeguards are in place to protect anonymity of voters in case of e-voting?
- 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?

[23] See: https://cdt.org/insight/election-cybersecurity-101-field-guide-ddos-attack-mitigation/
[24] See: https://www.cyberscoop.com/swiss-voting-system-flaw-encryption/

- What are the mechanisms available to monitor, detect and respond to cybersecurity attacks related to e-voting?
- Are there training provided on cybersecurity for those involved in elections?

1.3 The role of the Election Management Body

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. They need expertise in data protection as well as in cybersecurity.

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

As noted by the European Data Protection Supervisor, "data protection law, electoral law and audio-visual law share common principles, such as transparency and fairness, and cooperation between the respective regulators, especially during the electoral period, could enhance their coherent application and strengthen the protection of individuals against potentially unfair microtargeting practices." This cooperation has so far often been lacking.[25]

For the 2019 European Parliament election, rules were introduced to provide a mechanism for national data protection authorities (DPAs) to inform the Authority for European Political Parties and European Political Foundations of any decision finding an infringement of data protection rules where such infringement is linked to political activities with a view to influencing elections to the European Parliament.[26]

It is unlikely that left on their own, these different authorities will systematically cooperate. Instead, governments should consider setting up a coordinating mechanism, particularly in

[25] 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
[26] See https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

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.

Questions:

- Do EMBs have expertise in data protection and cybersecurity?
- 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 Complaints and redress

An independent complaint mechanism is necessary to ensure that electoral processes are free and fair and that all actors involved are accountable. As elections and democratic processes (such as participation in political campaigns) are manifestations of the enjoyment of fundamental human rights, governments have legally binding obligations to ensure that individuals have an effective right to redress any violations of their rights in this context.

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 capacity to receive complaints. At the very least, these authorities should have the mandate to receive any complaints related to abuse of personal information in the electoral context. For example, in Italy the DPA investigated the

'Rousseau' platform of the Five Star Movement[27] and in the UK, the DPA, fined the campaign group 'Vote Leave Limited' for sending thousands of unsolicited text messages in the run up to the 2016 EU referendum.

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 observers 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 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;
- 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.

[27] https://privacyinternational.org/examples/2843/failures-five-star-movements-rousseau

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?
- Do the ERB accept complaints by individuals and organisations?
- What are the remedies available (fines, imposition of conditions or restrictions in the processing of personal data, etc.)?

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. Further it is becoming clear that rules regulating political campaigns have not kept up with the current means of campaigning, particularly the growing reliance on digital communications and social media.

As the European Commission starkly noted in 2018: "Online activities, including during the election processes, are developing fast, and thus increased security and a level political playing field are key. Conventional ("off-line") electoral safeguards, such as rules applicable to political communications during election periods, transparency of and limits to electoral spending, respect for silence periods and equal treatment of candidates should also apply online. […] This is not the case now, and that needs to be remedied […]".[28]

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 – where political parties are creating their own datasets – as political intelligence – to help

[28] See: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-free-fair-elections-communication-637_en.pdf

inform campaign strategies and test and adapt campaign messaging – and finally, as political influence.[29]

Applying data protection safeguards to the personal information used by political parties is key to avoiding abuses which can potentially undermine democracy and the holding of free and fair elections.[30]

Personal data revealing political opinions is a special category of data under the modern data protection laws, such as the EU General Data Protection Regulation. As a general principle, the processing of such data is prohibited, with narrowly-interpreted exceptions, such as the explicit, specific, fully-informed, and freely-given consent of the individuals' affected.

Further, personal data which have been made public, or otherwise been shared by individual voters with political parties, even if they are not data revealing political opinions, are still subject to, and protected, by data protection law. As an example, personal data collected through social media cannot used without complying with the obligations concerning transparency, purpose specification, and lawfulness.

The risk that abuses of personal data may affect democratic elections motivated the EU to introduce measures, including a sanctions regime, in the May 2019 elections for the European Parliament. As noted by the European Commission, "it should be possible to impose sanctions on political parties or political foundations that take advantage of infringements of data protection rules with a view to deliberately influencing the outcome of elections to the European Parliament."[31]

Despite these risks, even recent data protection laws sometimes include exemptions to the data protection requirements for political parties. These exemptions risk undermining efforts to address the risks of exploitation of data during elections.[32]

For example, in Spain, a provision in the Spanish data protection law provided an exemption for political parties.[33] The Spanish DPA argued for a restrictive interpretation and the

[29] See Information Commissioner's Office, Democracy Disrupted?, 11 July 2018, https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf
[30] See: https://privacyinternational.org/long-read/2850/data-exploitation-and-democratic-societies
[31] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf
[32] See: https://www.gdprtoday.org/gdpr-loopholes-facilitate-data-exploitation-by-political-parties/
[33] See: https://privacyinternational.org/long-read/2821/spanish-elections-under-new-data-protection-law-use-personal-data-political-parties

Ombudsman (Defensor del Pueblo) brought a legal challenge, following which in May 2019, the Constitutional Court declared the provision unconstitutional.[34]

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 through platforms like WhatsApp);
    - 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);
    - facilitate the exercise of data rights by individuals (including providing information about how their data is processed and providing access to it); and
    - ensure that any third parties they are using for their campaign activities also comply with data protection laws.

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 they disclose where they get the personal data and what they do with it?
- Do they carry out data protection impact assessments relating to their processing of personal data?

[34] See: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_074/Press%20Release%20No.%2074.2019.pdf and https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/Press%20Release%20No.%2076.2019.pdf

- Have they obtained consent for the individuals or how else do they justify holding the data?

2.2 Political campaigns

Political campaigns around the world have turned into sophisticated data operations. The Cambridge Analytica scandal, while not unique, raised awareness about the potential impact of the combination of micro profiling and powerful machine learning on electoral processes.[35]

The European Data Protection Board summarised neatly the role of personal data in modern political campaigns: "Political parties, political coalitions and candidates increasingly rely on personal data and sophisticated profiling techniques to monitor and target voters and opinion leaders. In practice, individuals receive highly personalised messages and information, especially on social media platforms, on the basis of personal interests, lifestyle habits and values."[36]

Profiling and data-driven targeting techniques used by the broader digital advertising industry are increasingly deployed in the political campaigning context.[37] Various companies offer specific services tailored to elections context.[38]

- *Profiling*

Profiling is a way to collect, derive, infer, or predict information about individuals and groups, personal preferences, interests, economic situation, etc.[39] Such knowledge can be used to

[35] 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.

[36] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

[37] 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 7 April 2019].

[38] Oracle Data CloudData Directory; Experian Marketing Services, A Reference Guide to All the Ways Experian Can Help Your Marketing Efforts, White Paper.See particularly one of Experian marketing services that apparently can influence voters behaviour: OmniActivation Strategic Services, Data, Targeting and Measurement: Full-Service Digital Display Campaigns Run by the Experts, Product Sheet, Experian.

[39] GDPR defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;" Article 4(4), EU Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard

make or inform decisions, score, rank, evaluate, and assess people, and to make or inform a decision that personalises an individual's environment.[40] 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[41] 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'.[42] 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".[43]

- *Data-driven Targeting Techniques*

Profiling enhances and improves various data-driven targeting techniques, including the following, among others. **Micro-targeting** individual voters allows political actors to send personalised messages – on the basis of provided or inferred preferences – through online services such as social media platforms.[44] Another targeting method is **geo-fencing**, where individuals are dynamically targeted on the basis of their location.[45] **'Search influence'**, also, helps political parties and other actors to optimise and increase online research rankings, particularly at local search results. These are data-driven targeting techniques that are increasingly used to target voters and influence their actions. The use of these techniques facilitates the creation of information filter bubbles of interests for political campaigning that are also used to spread misinformation intended to amplify social divisions and manipulate the actions of specific individuals or groups.[46]

---

to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016.

[40] Kaltheuner and Bietti, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR', 2 Journal of Information Rights, Policy and Practice (2018), available at https://jirpp.winchesteruniversitypress.org/article/10.21039/irpandp.v2i2.45/ (last visited 4 April 2019).

[41] Privacy International, A Snapshot of Corporate Profiling, 9 April 2018, available at http://privacyinternational.org/feature/1721/snapshot-corporate-profiling (last visited 4 April 2019]. Our Complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad, 8 November 2018, Privacy International, available at http://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad (last visited 7 April 2019).

[42] Democracy Disrupted? Personal Information and Political Influence, Information Commissioner's Office, 11 July 2018, p. 36.

[43] Winterberry Group Report: "Know Your Audience: The Evolution of Identity in a Consumer-Centric Marketplace", August 2018 https://www.winterberrygroup.com/our-insights/know-your-audience-evolution-identity-consumer-centric-marketplace

[44] D. Ghosh, What Is Microtargeting and What Is It Doing in Our Politics?, 4 October 2018, Internet Citizen, available at https://blog.mozilla.org/internetcitizen/2018/10/04/microtargeting-dipayan-ghosh.

[45] More broadly on geo-targeting see, "Geotargeting: The Political Value of Your Location", Tactical Tech, available at https://ourdataourselves.tacticaltech.org/posts/geotargeting/.

[46] See: https://ourdataourselves.tacticaltech.org/projects/data-and-politics/

It is important to recognise that these 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 political manipulation and disinformation happens at all times, and not just around elections. [47] In Privacy International's view, regulation of the use of data for political campaigning should not be time limited to the election period.

Additionally, there is a plethora of companies and other actors, beyond political parties and official 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 and growing phenomenon, which directly influences democracy.

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.
- 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.
- 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

[47] E.g. in the UK context: https://www.politico.eu/article/britain-nationalist-dark-web-populism-tommy-robinson and https://www.theguardian.com/politics/2019/apr/03/grassroots-facebook-brexit-ads-secretly-run-by-staff-of-lynton-crosby-firm.

the right to information 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?
- 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. Even more, recent and on-going investigations have shown how the traditional rules of campaign financing fail to regulate and shed a light on these new forms of online fundraising and expenditures.

In the UK, for example, the Electoral Commission investigated the Vote Leave campaign,.[48] In July 2018, the Electoral Commission determined that five payments various Leave campaign groups made to a Canadian data analytics firm, AggregateIQ, violated campaign funding and spending laws. The Electoral Commission fined 'Vote Leave' and referred them to the police for breaking electoral law. The Electoral Commission has called for changes in the laws to increase transparency for voters in digital campaigning, including on spend.[49]

In its 2018 report on online manipulation and personal data, the European Data Protection Supervisor noted that "the reported spending on campaign materials may not provide sufficient details about spending on digital advertising and associated services, e.g. targeted ads on social media, analytics services, creation of voter databases, engagement with data brokers."[50]

Recommendations:

- Campaign finance laws should require timely reporting on spending on online campaigning and on the funding obtained on-line. The information should be sufficiently granular and detailed to promote transparency and accountability.
- 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 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

[48] https://www.electoralcommission.org.uk/i-am-a/journalist/electoral-commission-media-centre/party-and-election-finance-to-keep/leave.eu-fined-for-multiple-breaches-of-electoral-law-following-investigation
[49] https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf
[50] 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

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 amount paid on online political advertisements? What are the details of such disclosure (e.g. disaggregated by digital platforms; etc.)?
- 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. These concerns are heightened closer to elections periods, but they are relevant anytime given how even seemingly non-political online context can result in the mobilisation of people politically

3.1 The 'scarcity' assumption

One of the key campaigning safeguards 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 is assumed, would not apply to online media, given the facility and variety of sources of opinions and access to them.

However, this assumption does not take into consideration the market concentration 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.)

A few tech giant companies act as gatekeepers of the digital content which most individuals access online. As noted by the European Data Protection Supervisor, "data analytics could help individuals navigate through the increasingly noisy information environment" but "in effect, the forum for public discourse and the available space for freedom of speech is now bounded by the profit motives of powerful private companies".[51]

In particular, search engines and social media platforms filter the news and opinions users can access based on profiling. Profiling is relying on processing of information to evaluate, analyse and predict personal information, often in ways which are beyond users' understanding (see section 2.2 above.) This goes beyond paid-for targeted advertisements and promotion of content[52] to the way all content is displayed and recommended.[53]

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.

[51] 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
[52] See for example, criticism of the implications of Facebook's control on the promotion of political content in Hungary https://www.theguardian.com/world/2019/may/18/hungary-crucible-facebook-attempt-banish-fake-news
[53] 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

are direct consequences of profiling and have significant effects on the formation of political opinions and ultimately on elections.

Recommendations:

- Internet and social media platforms must be transparent about their profiling activities, including for the personalisation of what people see. This is of heightened importance during the electoral period.
- 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 and targeting services work? Who can access those services?
- Do the platforms comply with national data protection legislation or any regional standards (e.g. GDPR)?
- Doe the major platforms have an in-country contact person? What mechanism is available for reporting abuse and addressing complaints?

3.2 Transparency of online political ads and issue-based ads

Political parties and other actors target voters using not only data they collect themselves (see above, section 2), but also use tools that social media platforms provide to infer more data and to expand their reach and target other individuals, for instance through lookalike audiences.[54] Social media platforms share responsibility with political parties and other actors for the way personal data is used to target individuals.

Lack of transparency and more broadly lack of adequate regulation of online political ads have become a major concern during elections.

Recent initiatives by the European Union[55] and by certain states (e.g. Canada,[56] the US,[57] and Ireland.[58]) have sought to fill this lack of regulation by imposing – or, in the case of the European Commission Code of Practice on Disinformation, encouraging – transparency obligations on search engines, social media and other companies.

While imperfect, these transparency measures can improve the capacity of independent researchers and civil society organisations to monitor the impact of political ads and issue-based ads in election campaigns.[59] Election observers could also benefit from this transparency as they conduct assessment 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.
- Internet platforms, including search engines and social media platforms, should publicly disclose all advertising including political advertising and political issue-

[54] This was used by the far-right AfD in Germany (https://www.bloomberg.com/news/articles/2017-09-29/the-german-far-right-finds- friends-through-facebook) and is explained further here (https://policyreview.info/articles/analysis/role-digital-marketing-political-campaigns).
[55] See: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation
[56] See: https://policyoptions.irpp.org/magazines/april-2019/learned-googles-political-ad-pullout/
[57] See proposal for a Honest Ads Act: https://www.congress.gov/bill/115th-congress/senate-bill/1989
[58] See the Private Member's Bill, Online Advertising and Social Media (Transparency) Bill 2017, https://www.oireachtas.ie/en/bills/bill/2017/150/?tab=bill-text
[59] See for example: https://newsroom.fb.com/news/2019/04/election-research-grants/, https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/, https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadequate/

based advertising. Disclosure should at least include targeting parameters (intended audience, actual audience, profiles) and who paid for the ads.

- 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 advertisement and issue-based advertisement 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 to monitor and review the ads in the run up to the election?

Conclusions

Digital technologies are changing the way elections and political campaigns are run. They open new opportunities to engage with voters and to support voters' participations in elections and in democratic processes. They also raise novel issues and challenges for all electoral stakeholders.

In particular they demand changes in laws and practices to ensure elections are free, fair and transparent, and that the actors involved are held accountable. Because of the role played by data in the digital environment, privacy, data protection, including cyber security of the electoral processes, are central to these reforms.

Election observer organisations have a fundamental role to play to ensure that 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 digital technologies and to provide remedial recommendations.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org