European Parliament

Artificial intelligence, data protection and elections

The Facebook/Cambridge Analytica case in 2018, revealing alleged misuse of personal data for political advertising, demonstrated how the underlying values of the European data protection rules are essential for democracy. The EU has recently adopted a series of additional initiatives to support free and fair elections, reflected not least in European Parliament (EP) debates and resolutions.

Personal data and data analytics

Every day, most of us use digital devices, searching or posting online, and produce considerable amounts of data, capable of revealing, with the help of algorithms and data analytics, information about how we think and feel. It is said that 'we are data', as the digital profiles so created can be used to predict our behaviour and personalise the services accessed. Data protection rules are in place to reduce the risks of improper use, of which the user is often unaware. When the purpose of the personal and behavioural data collected is to filter the content users can see, to influence their opinions or even to target them as voters, the issue at stake is nothing less than the democratic system itself.

The right to data protection is recognised for **everyone** in Article 8 of the Charter of Fundamental Rights (CFR), binding as EU primary law since the Lisbon Treaty, and in Article 16 TFEU. Data must be processed fairly and for specified purposes, based on the subject's consent or other legitimate grounds laid down by law. Compliance with the rules is subject to control by an independent authority. Building on its 1995 predecessor and on the jurisprudence of the EU Court of Justice, the GDPR is fully applicable since 2018, with the aim of strengthening rights and fostering trust in the digital age.

The Facebook and Cambridge Analytica case

In 2018, newspapers reported that a UK-based political consulting firm, Cambridge Analytica (CA), had improperly obtained data on 87 million Facebook (FB) users (including 2.7 million Europeans), without their consent. Data collection was initially made via a third-party application that 270 000 FB users were invited to install (voluntarily) for research purposes. Data of friends of friends, collected exponentially, were passed to CA, which used that data to target online voters/users with personalised political ads, allegedly seeking to manipulate their behaviour in the 2016 UK and US polls. Afterwards, FB announced it had made changes to restrict app developers' access to data, and CA shut down in 2018. However, the connections between unlawful data processing and disinformation/manipulation of data revealed have raised criticism in Europe.

Initial reactions. EU institutions recognised the relevance of data protection, and promised to leverage the provisions of the GDPR. A heated debate took place in the European Parliament plenary in April 2018. Members called for a strong European position, stressing the role of data protection as a line of defence against election manipulation: Members expressed concerns regarding the risks that the democratic process may suffer if data are used to manipulate political opinion or voting choices. While the European data protection authorities established a Social Media Working Group, the European Data Protection Supervisor issued an Opinion on online manipulation, stressing that the scandal is a symptom of a predominant business model, and that relying on the goodwill of tech companies is not enough. For some experts the big change would be around enforcement of the data protection rules: Europe would need to 'show its teeth' in imposing compliance (e.g. on limitations to automated profiling). Investigations and sanctions at national level have also been undertaken.

The European Parliament: A long tradition of supporting data protection

As part of its varied powers, also widely exercised in the data protection field, the EP has been active in investigating the scandal of Facebook/CA – which are companies certified under the EU-US data transfer deal, the Privacy Shield. The EP adopted a resolution in July 2018 on the (in)adequate protection afforded by the Shield to guarantee European users' rights, and called on the European Commission to suspend the

Author: Shara Monteleone, Members' Research Service

PE 637.952 – May 2019

agreement. Moreover, a series of hearings were organised to assess the impact of the Facebook/CA case, and FB CEO Mark Zuckerberg was invited to meet EP Members, although the answers provided were unsatisfactory.

An EP resolution, adopted in October 2018 on the use of FB users' data by CA, urges Member States to engage with online platforms to increase awareness and transparency regarding elections.

Micro-targeting, disinformation campaigns and data surveillance

While micro-targeting for political campaigns may simply be seen as commercial advertising, it may threaten democracy, public debate and voters' choices substantially when the related practices rely on the collection and manipulation of users' data (big data analytics) to anticipate and influence their political opinions and election results (computational propaganda). While GDPR is considered a strong instrument to ensure digital technologies are consistent with democratic values, it may not be sufficient alone.

A social media post says a lot about us. As we live in what has been defined as a black box society, our behaviours, preferences and the related data become (through clicks) (freely) available to large, commercial technology companies (also defined as 'surveillance capitalists' due to the market concentration created), creating a vulnerability in both our digital and real lives. Such companies could develop methods capable not only of automating and translating every activity into data, but also capturing the *surplus* of personal data, to make users uncover data that they would otherwise not provide, and to transfer this knowledge into power. For these reasons, privacy and competition laws must be considered as intertwined. A behaviour, or a decision, can be manipulated in a certain way for commercial aims, but also for political outcomes, often without the users' awareness or choice. Such concerns may rise, given the increased availability to some of these companies of surveillance tolls (traditionally used by intelligence services).

EU Voice

The European Parliament has consistently investigated such disinformation and unlawful data processing and urged a strong and coordinated European response. The measures adopted at the EU level in 2018 include: the Commission's communication on 'Tackling online disinformation', supporting a European approach; the creation of an independent European network of fact-checkers; the Code of Practice on Disinformation, signed by several online platforms: a self-regulatory tool, which should improve transparency on the origin of the news, on how it is sponsored and targeted, and should also help with concrete actions in view of the elections. As a result, Facebook recently launched transparency rules.

While elections remain primarily a Member State responsibility, a package on free and fair European elections was adopted to protect the electoral process from disinformation campaigns based on the misuse of voters' data, including: financial sanctions (signed in March 2019) for European political parties in case of deliberate infringement of data protection rules to influence EU elections (i.e. taking advantage of unlawful data processing); a recommendation for Member States to cooperate in securing the European elections; and guidance on the application of data protection law in the electoral context.

Artificial intelligence, data protection and elections

Given their popularity, all European political parties currently use online social media for electoral campaigning. However, the lawfulness of some parties' data collection and use remains questionable.

Technological possibilities may enhance or undermine political decision-making. As there is a strong relationship between digital technology, democracy and polarisation of public discourse (a user is exposed to a one-sided set of information), its design impacts participation, debate and democracy.

It is clearer than ever that, while privacy and data protection are essential for other rights and freedoms (of thought, of choice, of movement), the use of new, often-opaque, automated decision-making practices, relying on algorithms, requires higher transparency, as well as joint accountability on the part of different actors, and ethical considerations. The European Data Protection Supervisor (working with other EU bodies to ensure that data are used responsibly and that voter rights are respected), stressed that data protection is a prerequisite for fair and democratic elections, and called for regulators (electoral, media, data protection authorities) to make a joint effort to protect election integrity.