PERSONAL DATA WAS WEAPONISED AGAINST DEMOCRACY IN THE EU - AND CAN BE AGAIN

-

04.04.2018

EurActiv (4 April 2018)

With the recent revelations on the unlawful use of voters data to influence their choices, both the EU and its member states need to take legislative measures to prevent such campaigning, which violated privacy rights and eroded democracy. The first step should be to end the lack of transparency, writes Nomi Byström.

Nomi Byström is a postdoctoral researcher in computer sciences at Aalto University, Finland.

Whistleblower Christopher Wylies revelations on the exploiting of voters data have been heavyweight not once but twice. In the European Union too, personal data of millions was harnessed to influence choices at the ballot box: to vote for leaving the European Union in the Brexit referendum of 23 June 2016. As for voters themselves, they were oblivious to what was done with their information.

But Wylies insights also affirm how truth can be stranger than fiction. Perhaps this is also the reason why, despite attempts to draw attention to the abuses of data for years, scholars, journalists and civil society organisations have had an uphill struggle to make their voices heard.

The March revelations did not come out of the blue. Rather, they have brought much-needed attention to what has been known about shady and nothing short of unlawful campaigning activities.

Violating the UK Data Protection Act, enormous, politically significant databases were created and voters were targeted billions of times in the run-up to the referendum. It can only be hoped, to borrow Carole Cadwalladr of the Observer, that a public inquiry is held in England.

In addition to the campaigns and companies, it should include an examination of the extensive foreign involvement.

Significantly, the EU Parliament will also be investigating. However, that is no longer enough.

Both the Union and member states need to take legislative measures against a repetition of campaigning that both violated privacy rights and eroded democracy, a fundamental value found in Article 2 of the Treaty on European Union.

Expectations that the General Data Protection Regulation will single-handedly tackle harvesting of personal data to win at any cost at the ballot box are unrealistic. True, the GDPR does have sharp

teeth with its administrative sanctions (up to 20,000,000 EUR or 4% of the total worldwide annual turnover), but a much-needed algorithmic bite is missing. And its Article 22 is limited to a decision based solely on automated processing.

Psychological manipulation of voters with their own personal data has become a threat to democracy. In addition to data protection, campaign financing and other rules may be ignored to intensify the personalised targeting.

First, the lack of transparency has to come to an end. The secretiveness of the entire scope of data processing; unavailable algorithms and closed proprietary platforms where the interference has been carried out have had damaging consequences.

In addition to facilitating unlawful practices, they have hindered an open, constructive political debate and boosted extreme emotional material with little regard for the truthfulness of the content.

Transparency and effective oversight need to begin with, but not be limited to, Facebook. It should no longer be permitted to hide behind cosmetic improvements and polite apologies. Self-regulation has led to no regulation.

Campaigning and companies that disregard the law have to be made accountable. Fines alone are no deterrent. Rather, they favour wealthier candidates and their superrich backers.

Political consulting, data analytics and digital advertising companies that engage in illegal hacking practices and intimidating, indoctrinating or threatening voters anywhere in the world should not be permitted to operate in the Union.

Last but not least, measures are required to tackle how foreign actors, typically beneath the radar, can become involved in national or EU Parliament elections in a variety of means, for example, building huge databases of voters, manipulating them from abroad, creating shell companies or with services and donations.

Motives, in addition to undermining democratic institutions and destabilising society, include impacting how a country is run to advance own political goals.

Electoral campaigning has been massively disrupted, not least with data science. Yet the pertinent laws and powers of authorities may not even have caught up with digitalisation. To borrow the words of Vote Leaves campaign director, The law/regulatory agencies are such a joke the reality is that anybody who wanted to cheat the law could do it easily without people realising.

And still, with the advances in machine learning, there is no longer even the need for the psychographics employed earlier by Cambridge Analytica. Voters can be subjected to relentless real-time surveillance, followed by ever-evolving, ever-more invasive and tailor-made manipulation.

At the same time, the surge in data is only beginning. The IoT (Internet of Things) revolution is knocking on the door. When not already today, soon everything from connected pills, beds, mirrors, digital assistants, condoms, plates, jeans and heating systems to entire homes will be transmitting information about their users.

That data is invaluable to those seeking comprehensive insight into voters life and, in particular, vulnerabilities.

Remaining inactive or settling for voluntary, unenforceable codes of conduct will only risk a repetition of the 2016 vote. It undermined democracy and changed the future course of both the UK and the entire European Union.

Kaynak/Source: