HISAR SCHOOL
JUNIOR MODEL UNITED NATIONS 2025

Protecting Democracy in an Age of Severe Political Polarization and Extremism by promoting constructive discourse

SA5: CYBER CRIMES

Limiting data exploitation of individuals during times of democratic elections

DERIN ŞENER

RESEARCH REPORT

Forum: Cyber Crimes (SA5)

Issue: Limiting data exploitation of individuals during times of democratic elections.

Student Officer: Derin Şener- President Chair

Introduction

In the digital age, the exploitation of personal data for political purposes has become a widespread concern, particularly during democratic elections. Data exploitation refers to collecting, processing, and misusing individuals' personal information, often without their knowledge or consent, to manipulate public opinion. Political parties, governments, and private companies have repeatedly used data-driven strategies to influence election outcomes by targeting specific voters with tailored political ads, messaging, and disinformation campaigns.

The issue poses a direct threat to the integrity of democratic processes. It weakens election transparency and can affect voter behavior, ultimately affecting electoral results. This problem is closely linked to the theme of democratic integrity and ethical governance. Data exploitation not only breaches individuals' right to privacy but also challenges fundamental democratic principles, making it an urgent issue to address.

Definition of Key Terms

Data Exploitation: The unethical or unauthorized use of personal data, often involving the collection, analysis, and sharing of information without the individual's informed consent. This term is typically used in the context of privacy violations and unethical practices.

Big Data: Refers to large, complex data sets that can be analyzed computationally to reveal patterns, trends, and associations, particularly relating to human behavior and interactions.

Micro-targeting: A marketing strategy used in political campaigns to send tailored messages to specific groups of voters based on detailed profiles, often created using personal data such as browsing habits, voting history, and social media activity.

Algorithmic Manipulation: The process by which algorithms, designed to process and analyze data, are used to influence user behavior in ways that may not be transparent. This may involve manipulating voters' opinions through targeted advertisements and disinformation in elections.

General Overview

The rapid expansion of digital technologies has changed political campaigning, with the collection and exploitation of personal data at the center of modern election strategies. During election periods, political parties and interest groups often utilize data obtained from social media platforms, data brokers, and online tracking to create detailed voter profiles. These profiles enable micro-targeting, where specific political messages are delivered to individuals based on their preferences, opinions, and even psychological traits.

In the past, the misuse of voter data was not a prominent issue, as most campaigning was done through traditional media such as television and newspapers, which does not involve personal data. However, the rise of the internet, social media, and big data analytics has enabled vast exploitation and manipulation. For example, in the 2016 US Presidential Election and the UK's Brexit referendum, the data of millions of Facebook users was harvested without consent by the political consulting firm Cambridge Analytica. This data was then used to create targeted campaigns aiming to influence voter behavior.

In the aftermath of these incidents, international organizations, governments, and civil society have expressed growing concern over the lack of transparency and regulation concerning the usage of personal data in elections. Countries have introduced various legal frameworks, such as the EU's GDPR, but the global nature of the internet means that national regulations are often insufficient to address international data flow and exploitation.

The need for stronger international cooperation and more robust legal mechanisms to prevent the exploitation of individuals' data is evident. Without further action, elections could become increasingly open to manipulation by private companies, foreign governments, and political actors who exploit data for their benefit, threatening the democratic process.

Major Parties Involved and Their Views

Social Media Companies: Social media companies such as Facebook, Twitter, and Google are crucial to the issue as they host the platforms where much of the data is collected and used. While social media platforms argue that they have implemented safeguards and transparency measures, they have also faced criticism for prioritizing their profit over users' privacy and failing to prevent data exploitation on their platforms.

Political Parties: Many political parties and candidates rely on data-driven strategies to win elections. Some parties argue that data use is a legitimate campaign tool for effectively reaching voters. However, others recognize the ethical concerns and support stricter regulations to ensure data exploitation does not undermine democratic fairness.

Data Brokers: Data brokers are companies such as Acxiom and Experian that specialize in collecting and selling large amounts of consumer data, including personal information, browsing history, and purchasing habits. They play a key role in enabling political campaigns to access detailed voter profiles, which can be used for targeted political ads.

International Organizations: International organizations such as the United Nations (UN) and the European Union (EU) have advocated for the establishment of international guidelines on data protection and privacy of elections. The EU's GDPR is a leading example of a comprehensive legal framework to protect individual data rights, but more work is needed globally.

Privacy Advocacy Groups: Organizations such as the Electronic Frontier Foundation and Privacy International campaign for stronger privacy protections and greater accountability for those who exploit individuals' data. They argue that individuals' data should not be used as a tool for political manipulation, and they call for transparency and informed consent as fundamental principles in data governance.

Timeline of Events

Date of Event	*Description of Event*
2013	*Edward Snowden reveals widespread government surveillance programs collecting personal data.*
2016	*Cambridge Analytica scandal: Data from millions of Facebook users exploited in the US election and Brexit.*
2018	*The European Union enacts the General Data Protection Regulation (GDPR), strengthening data privacy rights.*
2020	*Facebook and Twitter implement transparency measures for political ads after increased scrutiny.*
2023	*United Nations calls for international data privacy regulations, citing growing concerns over election interference.*

Treaties and Events

General Data Protection Regulation (GDPR)

Adopted in 2018, the GDPR is a landmark legal framework within the European Union designed to protect individuals' personal data. It requires companies to obtain explicit consent before collecting or processing data and imposes strict penalties for violations. While the GDPR has significantly improved data protection within Europe, its reach is limited to the EU thus making international enforcement challenging.

International Covenant on Civil and Political Rights (ICCPR)

While not focused specifically on data, the ICCPR protects individuals' right to privacy, which can be extended to cover data exploitation during elections. Articles 17 and 19 are relevant in discussions of privacy and freedom of information.

United Nations Guiding Principles on Business and Human Rights (UNGPs)

These non-binding principles outline the responsibilities of businesses, including technology companies, to respect human rights, including the right to privacy. They serve as a framework for addressing corporate responsibility in the digital age.

Evaluation of Previous Attempts to Resolve the Issue

Efforts to regulate data exploitation during elections have seen mixed results. The introduction of the GDPR in the European Union was significant in protecting individuals' privacy rights. It has forced companies to be more transparent about how they collect and use data and has given individuals more control over the personal information they possess. However, the GDPR is not a global solution, and many countries lack the regulatory procedures.

Social media companies have taken some voluntary steps to improve transparency in political advertising, such as creating ad libraries and labeling political ads. While these measures provide greater visibility, they do not fully address the issue of data exploitation. The many possible paths present for data exploitation make it difficult for countries and companies to implement effective protection methods.

Additionally, international efforts to establish a global framework for data privacy have been slow. Many conferencs and conventions have provided recommendations, but the lack of binding international agreements suggests that enforcement remains weak, mainly in countries with limited economic resources and political independence.

Possible Solutions

Governments and international organizations can collaborate to create a global regulatory framework that addresses data exploitation during election periods. This framework could establish minimum standards for data privacy, including requiring political parties and social media platforms to openly state how they use voter data. It could also establish penalties for companies that do not comply and create mechanisms for international enforcement.

Countries may update their national laws to include the growing effect of the misuse of personal data during elections. These laws should include provisions for voter data protection, requiring consent for data collection, and holding companies and political parties accountable for any breaches. Governments could also assign non-political observers to monitor data usage during elections.

Educational public awareness campaigns can also be useful for social media users to refrain from handing too much of their personal information to social media companies. A public awareness campaign on the importance of data privacy, particularly during elections, could help citizens better understand their rights and the risks associated with data exploitation. By educating voters on how their data is used, individuals would be more informed and be better able to protect their personal information from misuse.

Additional Resources

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2

https://gdpr.eu/what-is-gdpr/

https://www.nytimes.com/2018/05/24/technology/twitter-political-ad-restrictions.html

Bibliography

Here is the bibliography organized in alphabetical order:

Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." *The Guardian*, 17 Mar. 2018, www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Chester, Jeff. "The Role of Data-Driven Campaigning in Democratic Elections: Ethical Challenges and Solutions." *Journal of Information Technology & Politics*, vol. 17, no. 2, 2020, pp. 102-119.

European Union. *General Data Protection Regulation (GDPR)*. 2016. *EUR-Lex*, eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

Facebook, Inc. "Facebook Introduces Ad Transparency and Authenticity Measures Ahead of Elections." *Facebook Newsroom*, 27 Apr. 2018, newsroom.fb.com/news/2018/04/ad-transparency/.

González, Cédric, et al. "Data Privacy in Political Campaigning: An Overview of Current Practices and Regulations." *Computer Law & Security Review*, vol. 36, no. 5, 2020, pp. 1056-1070.

Hintz, Arne, et al. *Digital Citizenship in a Datafied Society: Civic Engagement and Data Privacy*. Polity Press, 2022.

Kreiss, Daniel, and Shannon C. McGregor. "The 'Arms Race' in Digital Campaigning: Data Analytics and Strategy in Political Elections." *Political Communication*, vol. 37, no. 1, 2020, pp. 34-55.

Solon, Olivia. "Twitter Launches New Ad Transparency Center to Show Who Is Behind Political Ads." *The Guardian*, 28 June 2018, www.theguardian.com/technology/2018/jun/28/twitter-political-ads-transparency-advertising.

United Nations. "Data Privacy, Ethics, and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda." *United Nations Global Pulse*, May 2018, www.unglobalpulse.org/document/data-privacy-ethics-and-protection-guidance-note-on-big-data-for-achievement-of-the-2030-agenda/.