ELECTION COMMISSION OF INDIA IN THE DATA-DRIVEN AGE

Shreya Shreekant, [BA LLB Hons., GNLU, LLM in Intellectual Property Law, Queen Mary University of London], Lecturer, at Jindal Global Law School.

ABSTRACT

This article aims to scrutinize issues and legal provisions that are likely to cause concern to voters in the current data-driven world. With India's data protection law framework still being in very nascent stage, it becomes imperative to look at loopholes in the existing draft bill and conduct of State to evaluate whether political manipulation of voters is possible or not. Central to democracy is free and fair elections and if loosely protected sensitive data of citizens can be misused to micro-target individuals into voter manipulation, it would sink our democratic electoral process.

The article seeks to discuss plausible issues that can arise in the electoral sector by studying the Personal Data Protection Bill, 2019 as well as recent electoral reforms and conduct of ECI.

Introduction

Every Indian citizen from their elementary education has heard about the saying (and a crucial fact) that--central to democracy, is free and fair elections. In a country as diverse and vast as India, this is a mammoth task. To make sure elections are conducted with true, secular, socialist, democratic perspective, Election Commission of India (ECI) has been given this gargantuan responsibility to make sure will of the people of India comes fore in the most fair manner possible.

Elections always loom large over political climate of any Nation. If not scrutinized by appropriate authorities, it has the ability to shake the very foundation most democratic countries are founded on. Indian Constitution (Articles 324 to 329) lays down provisions with respect to functioning and conduct of Elections by ECI. However, with time and digital evolution, like most things, conduct of elections has also evolved. The aim of this article is to study and analyze recent electoral trends, reforms and conduct in the digital, data driven world.

Over the last few years, election campaigning techniques have evolved from simple door-to-door canvassing to using data analytics technology to scrutinize voter opinion and behaviour. One of the most notorious electoral incidents of recent times is that of Cambridge Analytica where exploitation of personal data of US citizens via social media, led to massive breach of individual's privacy as well as massive political manipulation by microtargeting the voting population. Online surfing by people are integrated with publicly available electoral datasets to provide information age, caste, religion, political convictions and so on, which are then utilized to customize advertisements and other marketing tools to target voters. Moreover, with third parties like data brokers and data firms getting involved in the election process, the usual transparent facade of elections seems to be getting rather cloudy. The question amidst the rising concern over free and fair elections in this data driven world is, whether, the Indian electoral framework, existing data laws and proposed Personal Data Protection Bill, 2019 are enough to ensure truly successful elections to take place or not?[1]

How does data drive election campaigns?

Data driven election campaigns target voters' political beliefs and preference via accessing

[1] Shweta Reddy, *Data driven election campaigning and India's proposed data protection framework*, CIS, (Dec. 21, 2020), https://cis-india.org/internet-governance/blog/data-driven-election-campaigning-and-indias-proposed-data-protection-framework.

their personal data via social media and other internet applications. Massive amount of information ranging from age, religion, caste, gender to their preference for leaders, government policies, etc. are scrutinized. Such campaigns are contingent on ascertaining new and different sources of data that might allow political parties to examine voter preferences. Most details about an individual voter in such cases can be gathered from "publicly available" data on social networking websites or purchased from data brokers. Cookies, plugins and other tracking technologies can also be used. Eventually, all material collected is then utilized to profile and anticipate their political preference and accordingly target such voters with customized political advertisements. This is what leads to political manipulation of voters. Facebook likes have been found in studies to predict personality traits, political opinions, and other characteristics. However, the scope of such micro-targeting can vary and might not result in the most accurate results always.[2]

Is Indian data law and framework ready to avoid such 'political maneuvering' of voters?

The Personal Data Protection Bill of 2019 is the product of Supreme Court's 2017 verdict in the *Puttaswamy v. Union of India*[3] case, which recognized privacy as a fundamental right guaranteed by the Constitution of India.

The Joint Parliamentary Committee, which has been deliberating on the Bill since its introduction in Parliament in 2019, made several proposals for changes to the text of the Bill. However, it avoided amending the biggest problematic areas, such as the government's access to private data, which also invited dissent from opposition panel members. This Bill still stands pending today with the Standing Committee.

The Committee has retained Clause 35 of the Draft Bill. It gives the government the right to authorize any of its agencies to circumvent the provisions of the law if it finds it necessary to do so on grounds of "public order", "sovereignty", "friendly relations with foreign states" and "security of the state".

Clause 35 of the Bill states that, "*Where the Central Government is satisfied that it is necessary or expedient,—*

(i) in the interest of sovereignty and integrity of India, the security of the State, friendly

[2] *Id.*
[3] K.S. Puttaswamy v. Union of India, AIR 2017 SC 416.

relations with foreign States, public order; or

(ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order,

it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed."[4]

This clause can be easily construed as giving the Union complete discretion and authority to act as it wishes when it comes to accessing data of citizens. It permits the processing of personal data in the interests of state security in accordance with legal procedures which itself is not stipulated clearly. Moreover, it authorizes the use of personal data for the purposes of preventing, detecting, investigating, and prosecuting any crime or other violation of the law, which essentially leads to ambiguity while determining when exactly such *carte-blanche* techniques might be used against Indian citizens.

Given India's already lenient safeguards against state monitoring, the state's access to all personal data presents a substantial danger to the right to privacy. The governing standards for government surveillance in India is still being stipulated by precedent upheld in the *PUCL v. Union of India*[5], which was intended by the Supreme Court in 1996 as a temporary solution but appears to have been accepted permanently. The judgment concentrates authority in the hands of the executives to order and review monitoring without introducing judicial orders, any kind of third-party review, or any necessity to inform the subject of surveillance.

"*The PUCL Court notably declined to impose the procedural safeguard of prior judicial scrutiny (such as by the issuance of a warrant) for interception orders, which the petitioners had argued would be the only way to safeguard the right to privacy of an individual, as "judicial scrutiny alone would take away the apprehension of arbitrariness or unreasonableness […]". The Court's stated reason was that it could not require prior judicial*

[4] The Personal Data Protection Bill, 2019, Clause 35, Acts of Parliament, 2019 (India).
[5] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

scrutiny in the absence of a provision to that effect in the statute."[6]

The Committee received a lot of recommendations for amending this particular clause for obvious reasons. It also produced an excerpt from the *Puttaswamy* Judgment- "*The concerns expressed on behalf of the petitioners arising from the possibility of the State infringing the right to privacy can be met by the test suggested for limiting the discretion of the State:*

(i) The action must be sanctioned by law

(ii) The proposed action must be necessary in a democratic society for a legitimate aim

(iii) The extent of such interference must be proportionate to the need for such interference

(iv) *There must be procedural guarantees against abuse of such interference*"[7]

However, the Joint Committee Report, post suggesting three-fold requirement mentioned in the *Puttaswamy* judgment encapsulating Article 21, Article 14 and Proportionality requirements, it leaves upon the Government to frame the rules for oversight and safeguards for this provision.

The Committee did acknowledge that there is a possibility that the government might misuse data. Hence, they added a minor sub-clause in the report which suggests that government should exercise this provision only when it is just, fair and reasonable to do so.

What might be actions sanctioned by law which could invite such State scrutiny? What situations might warrant usage of such 'legitimate aim' term? Who defines Proportionality? These are the questions that arise in the minds of a cognizant person while perusing the current Data law proposed framework.

The draft bill today stands amended and includes "*for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order*" as part of Section 35 of the proposed legal framework. However, Section 36 which lays down further provisions for exemption of processing of data by State again postures ambiguous language which might raise challenging circumstances in future.

[6] Chaitanya Ramchandran, PUCL v. Union Of India Revisited: Why India's Surveillance Law Must Be Redesigned For The Digital Age, 7 NUJS L.Rev. 105 (2014), 109-110, http://nujslawreview.org/wp-content/uploads/2016/12/Chaitanya-Ramachandran.pdf.

[7] Joint Committee Report, Seventeenth Lok Sabha, *Report of The Joint Committee on the Personal Data Protection Bill, 2019*, ¶ 2.159, (December, 2021).

Therefore, the obvious question now is, whether ECI will be one of such agencies during elections, to be given free access to personal data to study voter behaviour by the State? Is there a risk from the side of incumbent governments to misuse such legal framework during elections?

Recently, a national party employed the method of using Voter Individual Profile (VIP) during Assam state Elections in order to alter campaigning that would most personally suit and align with the preferences of each individual. This method was carried out with the help of data consulting agencies that helped the Party in curating campaigns on the basis of personal information of the voter. While there is nothing essentially stopping the party from using legal means of collecting data, the fact that the government would keep personal information of the voter in its database for current and upcoming elections becomes a worrisome factor.[8] Thus, the Personal Data Protection Bill, 2019 is also required to include provisions which would curtail political parties and governments to be able to go to such lengths and infringe privacy of citizens.

Moreover, The Election Laws (Amendment) Bill, 2021 allows Electoral Registration officer to require voters to furnish their Aadhar card in order to establish their identity. This amendment brought said changes to Section 23 of the Representation of the People Act, 1950 and reads as follows:

"(4) The electoral registration officer may for the purpose of establishing the identity of any person require that such person may furnish the Aadhaar number given by the Unique Identification Authority of India as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016: Provided that the electoral registration officer may also require the Aadhaar number from persons already included in the electoral roll for the purposes of authentication of entries in electoral roll and to identify registration of name of the same person in the electoral roll of more than one constituency or more than once in the same constituency. (5) Every person whose name is included in the electoral roll may intimate his Aadhaar number to such authority in such form and manner as may be prescribed, on or before a date to be notified by the Central Government in the Official Gazette.

[8] Abbinaya Kuzhanthaivel, *How the BJP used big data to turn assam into a resounding success*, EAST MOJO (May 7, 2021) https://www.eastmojo.com/assam/2021/05/07/how-the-bjp-used-big-data-to-turn-assam-into-a-resounding-success/.

(6) No application for inclusion of name in the electoral roll shall be denied and no entries in the electoral roll shall be deleted for inability of an individual to furnish or intimate Aadhaar number due to such sufficient cause as may be prescribed: Provided that such individual may be allowed to furnish such other alternate documents as may be prescribed."[9]

Clause 4 of the Amendment provides for the Electoral Registration officer a method by law to demand Unique Identification Number of an enrolled voter. Aadhar was never meant as proof of citizenship which is why it is granted to all residents of India and not just citizens.

Clause 5 of the Amendment lays down a sort of a mandate for the individual voter to furnish their Aadhar number and Clause 6 aims at providing the individual a relaxation to Clause 4 for furnishing their Aadhar Card. However, this exemption comes tied with words 'sufficient cause', thereby, indicating that the individual will need to convince the Officer as to why Aadhar cannot be furnished and an alternative will be needed to be submitted in its absence.

By adding Clause 6 to Section 23 of The Representation of the People Act, 1950, the amendment bill introduces greater power being instilled in the hands of the Central Government. This leads one to wonder if the Government will have the discretionary power to decide whether a citizen, not holding an Aadhar should not be considered a valid voter?

Linking voter and Aadhaar databases could be deemed as an attack on the right to privacy of citizens. It raises grave concerns that such act on part of the government could violate our constitutional and fundamental right to secrecy of casting vote. India currently has no robust data protection law. Linking Aadhaar to the voter IDs would bring demographic information into the voter database. This would invite probability of increased surveillance, marginalization based on identity and targeted advertisements on the basis of sensitive private data. Recently, the Madras High Court asked the ECI to look into allegations against the Bharatiya Janata Party (BJP) illegally using Aadhaar data of voters in Puducherry for making political gains in the 2021 assembly election.[10]

An upsetting scenario could be that upon such linkage; since Aadhar is linked to a mobile

[9] The Election Laws (Amendment) Bill, 2021, Acts of Parliament, 2021.
[10] M.G. Devashayam, *Aadhaar linkage can sink India's electoral democracy – with voter profiling, selective exclusion*, THE PRINT (Dec. 24, 2021), https://theprint.in/opinion/aadhaar-linkage-can-sink-indias-electoral-democracy-with-voter-profiling-selective-exclusion/786812/.

phone, which in turn would be linked to social media, which is further linked to algorithms, which in turn are linked to user interests/views and could be at a much higher risk of voter behaviour policing/manipulation. With this step, voter profiling and targeted campaigns are all possible. Voter maniulation and probability of arbitrary disqualification of voters would be a lethal combination that could worsen India's electoral democracy.[11]

Voter Id linkage with the Aadhar card might seem like a small step towards more efficient administration and removal of fraudulent voters however, upon closer examination, the Electoral reform Bill might prove to be more harmful than helpful. Further, ECI introduced an app called 'cVIGIL' which stands for 'Citizens' Vigil'. This app aims to encourage voters to record illegal activities during polls by sending geo-tagged photos and videos to the ECI. The Election Commission had informed that it will "*hide the complainant's phone number and identity so as to encourage information against high and mighty without any risk of subsequent possible backlash.*"[12]

However, the aspect of geo-tagging, access to voter information, linking of algorithms with other social media networks and now inclusion of Aadhar biometrics and data not only puts fundamental right to privacy at risk, but also raises concern over concentration of such sheer quantity of sensitive data in the hands of one agency. It also poses significant queries whether our data protection framework, existing as well as proposed, is adept to deal with mammoth fundamental right issues that might occur in future or not.

[11] *Id.*

[12] Vasudha Venugopal, *Election Commission launches unique app for voters to report poll code violations*, ET (Jul. 03, 2018), https://economictimes.indiatimes.com/news/politics-and-nation/election-commission-launches-unique-app-for-voters-to-report-poll-code-violations/articleshow/64847025.cms?from=mdr.