VOLUME 15 ISSN 2456-9704

ALGORITHM, LAW AND DEMOCRACY

By Aastha Bansal and Srishti Nair
From Symbiosis Law School, Noida

Abstract
The next time you hear someone talking about algorithms, replace the term with "god" and ask yourself if the meaning changes (Ian Bogost,2015). We all use algorithms in our daily lives without even realising it: when changing a wheel, or when preparing a pancake from a recipe. These algorithms are no longer programmed line by line, but are now capable of learning, thereby continuously developing themselves (Emmanuel Letouzé, 2015). This paper will analyse how Algorithms though sounds like pinnacle of efficiency as they show us relevant content but how in turn, they are taking important decisions out of the hands of human. It will also analyse that how this process is affecting the politics in the country.

They are everywhere and yet the general public has a poor understanding about the sophisticated and insidious mechanisms used by these pre-programmed catastrophes creating system which often results in a blanket assumption that they are neutral in nature (Brey, 2005; Winner, 1980) thereby underestimating the powerful impact that they have on our lives. The two-fold aim of the paper is to right off the bat comprehend the ability of the manipulative nudging technique possessed by these algorithms to affect significant aspects of our everyday lives. Secondly to lay emphasis upon the growing need of algorithm regulation in view of the existing laws while concentrating on the impact that the European Union's General Data Protection Regulation of 2016 has on the routine use of machine learning algorithms and their governance across the world.

Keywords: Algorithmic bias, Democracy, machine learning, Algorithmic Accountability Bill,2019, Big-data.

"Algorithmic culture" is the use of computational processes to sort, classify, and hierarchize people, places, objects, and ideas.[1] The era of ubiquitous computing and big data is now firmly established, with more and more aspects of our everyday lives like play, consumption, work, travel, communication, domestic tasks, security, etc. being mediated, augmented, produced and regulated by digital devices and networked systems powered by software[2] it becomes important to understand what are algorithms and how algorithmic bias work.

What is Algorithm?

Software is fundamentally composed of algorithms – sets of defined steps structured to process instructions/data to produce an output.[3] Machine learning algorithms are trained based on datasets that are chosen by the programmers. With this training data, they recognize and leverage patterns,

[1] What is an Algorithm? , http://culturedigitally.org/2012/02/what-is-an-algorithm/, (last visited Aug 10, 2019).

[2] Rob Kitchin, *Thinking critically about and researching algorithms*, 20 ICS, 14–21 (2016).

[3] Algorithm [draft] [#digital keyword], http://culturedigitally.org/2014/06/algorithm-draft-digitalkeyword/, (last visited Aug 10, 2019).

associations, and correlations in the statistics. For example, an algorithm can be trained to distinguish between a horse and a donkey by being fed thousands of pictures of different horse and donkey. Classification is the easier of the tasks; applying an algorithm to a judgement call based on a human is much more multifaceted than that.

How does algorithmic bias work?

Now, we might think that algorithmic reasoning is rational and objective, regardless of the situation. As they record the information that we are feeding them and show us relevant results and advertisements according to our preferences and interests instead which is better than seeing something irrelevant or nothing at all. So, what us the need for us to be concerned about something which is meant to make our lives simpler? There is no denying that algorithms exercise power over us and there is general lack of understanding about how algorithms exercise their power over us. Thanks to explosion of big data[4] Algorithms are harnessing volumes of macro- and micro-data to influence decisions affecting people in a range of tasks, from making movie recommendations to helping banks determine the creditworthiness of individuals. In machine learning, algorithms rely on multiple data sets, or training data, that specifies what the correct outputs are for some people or objects. From that training data, it then learns a model which can be applied to other people or objects and make predictions about what the correct outputs should be for them. Therefore, these algorithms fed by big data can also amplify existing structural discrimination in society and can even seduce an electorate into false sense of security.[5]

This is precisely what happened when Amazon discovered that its internal recruiting tool was dismissing female candidates. Because it was trained on historical hiring decisions, which favoured men over women, it learned to do the same. Similarly, the types of cognitive bias that can be inadvertently applied to algorithms are stereotyping, bandwagon effects, confirmation bias, priming and selective perception.

Algorithms are taught to make predictions based on information fed to it and the patterns it extracts from this information. Given that humans show all types of biases, a dataset representative of the environment can learn these biases as well. In this sense, algorithms are like mirrors — the patterns they detect reflect the biases that exist in our society, both explicit and implicit.[6]

Microsoft unveiled Tay, a Twitter bot[7] that the company described as an experiment in "conversational understanding." The more you chat with Tay, said Microsoft, the smarter it gets, learning to engage people

[4] Big Data are extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions.

[5] Nicholas Diakopoulos & Sorelle Friedler, *How to Hold Algorithms Accountable*, MIT Tech Rev, https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/ (last visited Aug17, 2019).

[6] Nicole Kwan, *Hidden dangers in algorithms*, (Dec 2,2018), https://towardsdatascience.com/the-hidden-dangers-in-algorithmic-decision-making-27722d716a49.

[7] A bot (short for "robot") is an automated program that runs over the Internet. Some bots run automatically, while others only execute commands when they receive specific input.

through "casual and playful conversation. Within 24 hours the bot started tweeting racial slurs and comments like "Hitler was right, I hate Jews". This happened because the bot was trained to self-learn and in doing so it reflected the passive-aggressive, extremist views that exist on twitter.

Let us take example of America's criminal justice system, Judges there uses a risk assessment algorithm, which are designed to do one thing: take in the details of a defendant's profile and spit out a recidivism score[8]-to predict the likelihood an offender will commit further crimes, their flight risk, and a handful of other factors. These data points are then used to guide them in sentencing, bail, or whether to grant (or deny) parole. The problem here is that same risk assessment tools algorithms are trained on historical crime data. Therefore, the result produced was biased towards people of low-income group and black people.

How specifically it is posing threats to democracy?

Every generation has its own vision of dystopia, ours is the idea that Algorithms are taking decision making power out of the hands of humans. Facebook counts 2 billion users, Google represents 90% of global searches, Apple's market capitalization reached $1 trillion.[9] With these statistics, technologies ability to diffuse key messages and propaganda by vested interests cannot be undermined.

Twitter assumed centre stage in the Mexican political theatre in 2012. The failure of mainstream media to report on drug violence owing to threats from cartels had meant that Mexican citizens were already dependent on Twitter for news and updates.[10]

The 2017 French presidential elections showed just how extensive the use of bots can be. In May 2017, the Oxford Internet Institute conducted an analysis of the #Macron Leaks hashtag, which involved a data dump of the then presidential candidate's email correspondence. It found that 50 per cent of the Twitter content consisting of leaked documents and falsified reports was generated by only three per cent of the total number of Twitter accounts. These bot accounts were pushing out 1,500 unique tweets per hour garnering an average of 9,500 retweets. The study concluded that over 22.8 million Twitter users were exposed to this information every hour on election day in France.[11]

All of us might be aware of the Cambridge Analytical and Facebook hiatus but it's important to fully understand what happened. Cambridge Analytical is a political consulting firm based in the UK. According to their website they collect and connect data to strategically consult--and communicate--for and with political candidates. They stole the personal information of over 50 million Facebook users and they did this to create a system that could target US voters with

[8] Karen Hao, *AI sending people to jail and getting it wrong*, MIT Tech Rev, https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/, (last visited Aug 12, 2019)

[9] Pascal G. Bernard, *Is AI a threat to Democracy?* (May21,2019), https://towardsdatascience.com/is-ai-a-threat-to-democracy-4bef3e5fcfdd

[10] Anita Gurumurthy & Deepti Bharthur, *Democracy and the algorithmic turn*, Issue 27, IJHR, 1-4, https://sur.conectas.org/en/democracy-and-the-algorithmic-turn/.

[11] *Ibid.*

political advertisements curated to their psychological profile.

What may be inferred from the above discussion is that while data-based electioneering can potentially bring new effectiveness and efficiencies to organising and campaigning, the fact that the technological platforms that define the public sphere today are controlled by the elite does not bear well for the system of electoral democracy as a whole. In theory, the digital intelligence extracted from data cuts down human resource intensive work, allows for grassroot organizers to optimize their canvasing and mitigate the distortion of big capital in elections by allowing candidates to reach their constituencies over social media, at literally no cost. However, if the Cambridge Analytica or the Marcon Leaks episodes shows us anything, it is that we are headed for a vastly different future, one in which voter behaviour is being manipulated towards particular outcomes that may reflect neither a democratic mandate nor an informed choice.

Existing laws with regard to algorithmic regulations

The first name that occurs at the top of any list when canvassing for algorithm regulation is that of the EU data protection law for it is a rare example of such regulation operating which is available in legislative 'top-down' form and has the ability to be a possible model to be emulated[12].

The EU law makers took up the challenge of figuring out what rules should apply to ensure a functioning data protection system and how such rules should apply to algorithmic decision-making in order to ensure the constitutional guarantees such as the prohibition of discrimination[13] or the right to data protection[14]. In view of the same the new GDPR was framed and made applicable on member states in May 2018. The main objective was to adapt the previous data protection legislations to the challenges posed by more advanced technology, including self-learning algorithms, and harmonise the existing data protection rules all across the EU[15]. The General Data Protection Regulation, often described as a 'Copernican Revolution' in data protection law is a set of comprehensive regulations for the collection, storage and use of personal information of individuals[16]which seeks to bring into focus harmonization of the law and individual empowerment.

The GDPR replaced the 1995 Data Protection Directive while bringing with it well defined explicit jurisdiction, penalties as well as rights available to individuals.

Though GDPR does not directly address the issue of algorithm and AI, outlined below are certain provisions that address automated decision making and profiling and a number of provisions that will impact companies

[12] Lee A. Bygrave, *Algorithmic Regulation* (2017) https://www.kcl.ac.uk/law/research/centres/telos/assets/DP85-Algorithmic-Regulation-Sep-2017.pdf

[13] EU Charter of Fundamental Rights, art 21.

[14] Perel and Koren, *Black Box Tinkering*, n.4 (2017)3

[15] Merle Temme, *Algorithms and Transparency in View of the New General Data Protection Regulation*,4 EDPL (2017),473-485.

[16] Wolfgang Schulz & Stephan Dreyer, *The General Data Protection Regulation and Automated Decision Making- Will it deliver?*, Bertelsmann-stiftung *(2019)*, https://www.bertelsmann-stiftung.de/en/publications/publication/did/the-general-data-protection-regulation-and-automated-decision-making-will-it-deliver/

using artificial intelligence in their business activities.

Via Article 22 paragraph 1, the GDPR gives the data subjects[17] the right not to be subject to a pronouncement that is solely based on automated processing including that of personal data of an individual used to evaluate certain personal aspects of the said person, which has significant legal or similar effects on him or her. Exceptions to this provision include entering or performance of a contract or explicit consent of the data subject. Additionally, paragraph 71 of the preamble to the GDPR, which explains the rationale behind it explicitly requires data controllers to implement suitable technical and organizational measures that will help prevent, inter alia, discriminatory effects[18] based on processing of sensitive data. Further, the GDPR gives a 'right to explanation[19]' to the data subjects vide Article 13-15. This right ensures that the use of automated decision making shall be communicated to the data subject, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. It also attempts to ensure non- biased results via Article 9 and 22 which lays down guidelines with respect to processing of special categories of personal and sensitive data including data related to beliefs, culture, political opinions, ethnicity, gender orientation et. racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation etc.

Following the footsteps of EU, countries across the globe introduced their own set of regulatory frameworks including Algorithmic Accountability Bill (Draft) in the United States of America, Lei Geral de Proteção de Dados Pessoaisso in Brazil[20], HKMA guidelines in Hong Kong etc.by mirroring the ideas reflected in the GDPR.

On July 27, 2018, in light of the introduction of GDPR by EU, India also published a draft bill for a new, comprehensive data protection law to be called the "Personal Data Protection Act, 2018". The bill came into being after a nine- judge bench of Supreme Court of India in the case of Justice K. S. Puttaswamy (Retd.) v. Union of India and Others[21] decided that right to privacy to protection characteristically falls under the ambit of Right to life and personal liberty as ensured by Article 21 of the Indian Constitution. The Court opined that privacy protection allows a person to lead an existence of pride, without which the right to life and individual freedom would be good for nothing.

In its present state, the bill is applicable on the organizations involved in the below mentioned activities:

- Processing the data that has been collected, disclosed or shared within the territory of India.

[17] See Art. 4(1) GDPR

[18] Mario Martini, *Datenschutz Grundveror dnung, Bundes datenschutz gesetz* (Boris P. Paal & Daniel A. Pauly, 2nd ed., C.H. Beck 2018)

[19] Bryce Goodman & Seth Flaxman, *European Union Regulations on algorithmic decision-making, and a right to explanation,* AI MAGAZINE, at 51

[20] See Baker McKenzie, *10 Things You Need to Know About Brazilian General Data Protection Law* (December 11, 2018), https://www.bakermckenzie.com/en/insight/publications/2018/12/brazilian-general-data-protection-law

[21] 1 (2017) 10 SCC 1

- Processing the personal data that has a connection with any business carried on in the territory of India or has any connection with any activity which involves the profiling of data principles within the territory of India.

- Processing of personal data if the same is undertaken by the State, any Indian company or any Indian citizen or persons incorporated under the Indian law.

The draft bill and associated report were given by the Justice Srikrishna Committee and it constitutes within several provisions that impact agencies employing algorithm and attempts to account for accidental consequences of such developing technologies.

The bill defines harm including those associated with algorithmic infrastructure such as loss of work opportunities, biased treatment and denial of service[22]. Empowering the authorities to make explicit classes of huge damage could allow unexpected damages emerging out of utilization of innovation to be incorporated under the ambit of the bill. Like GDPR, it provides the individuals with a certain set of rights including the right to confirmation and access, correction, data portability, and right to be forgotten[23]. However, at the same time the Bill is deliberately silent on the rights and commitments that have been fused into the GDPR that address mechanized decision making including :The right to object to processing[24], the right to opt out of automated decision making[25], and the obligation on the data controller to inform the individual about the use of automated decision making and basic information regarding the logic and impact of same.

Further, to forestall predisposed results and place the interest of data principle first, the bill requires that data fiduciaries take measures to guarantee that individual information that is handled is complete, precise, not misdirecting and updated as for the reasons for which it is prepared. The interest of the data principal should be represented at every stage and to ensure the same, processing of personal data should be done in a transparent, fair and reasonable manner while being in accordance with the commercially accepted or certified standards.

Globally, each and every company can be subjected to the Indian Personal Data Protection Act, the GDPR and other privacy laws, if they gather or process personal data from these countries or within these countries. The only possible way to escape the duties and liabilities imposed under such acts is to stop business in the said territories. However, keeping in mind the size of economies and abundance of market opportunities provided by the countries like India and those of Europe, it is not a viable option for most multinational companies but neither is complete abandonment of algorithmic infrastructure. Prima facie it seems that the lack of any other choice will result in multinational companies following the set regulations thereby, providing blanket protection to the consumers. However,

[22] Amber Sinha and Elonnai Hickok, *The Srikrishna Committee Data Protection Bill and Artificial Intelligence in India,* (2018), https://cis-india.org/internet-governance/blog/the-srikrishna-committee-data-protection-bill-and-artificial-intelligence-in-india

[23] See Art.22 GDPR

[24] See Art. 21 GDPR

[25] *Supra* 23

certain inherent, unaddressed loopholes within these regulations create a black hole in the assumed blanket protection being provided thus, allowing infiltration into the rights of the people as well as the society as a whole.

The GDPR ensures transparency and accountability vis-a-vis the 'Right to Explanation[26]'. However, one of the major contentions to this right has been whether or not it has adequate legal backing. Goodman and Flaxman in one of their short paper in 2016, first talked about the creation of right to explanation but never did they elaborate upon the legal basis they see for this right. Except for Recital 71, there is no explicit mention of any right to obtain explanation. Other articles of the GDPR are vague, inconclusive and unclear with respect to the extent of human participation in automated processing[27]. Further, a closer reading of the text along with the drafting history indicates that presently, the document does not contain such a right and that we cannot simply read it into the regulation[28].

Another, contention is with respect to the extent of power gained over generation and application of algorithms vide Article 22. Article 22 much like its predecessor still involves fulfilling multiple criteria's[29] and massive derogation its rights which can lead to lower level of protection for individuals especially in light of banks, insurance companies, online service providers etc. Simultaneously, these exemptions open up a plausibility for noteworthy deviations between national regulatory frameworks for mechanized decision making, thus discouraging the harmonisation objectives of the regulations. Moreover, it fails to address important issues like that of opacity, data quality and learning algorithms which are factors that should have been essentially considered while evolving algorithmic governing laws.

The Personal Data Protection Bill draft that has been proposed also has its own set of loopholes. The bill brings in mandatory localisation of data[30] for which companies will have to shell out lump sum amount of money from their pockets for no purpose at all thus resulting in creation of a trade barrier for smaller players. Moreover, the bill grants excessive power to the centre via Section 98 along with a cart blanche right to non-consensual processing of personal information for any state function authorised by law[31].

AI systems can directly abet domestic control and surveillance, helping internal security forces process massive amount of data-including information shared on social media but giving such unfettered power to government in this respect is problematic. For instance, the Chinese government has used AI in wide-scale crackdowns in regions that are home to ethnic minorities with China. Surveillance systems in Xinjiang and Tibet have been described as "Orwellian'. These efforts have included mandatory DNA samples, Wi-Fi network monitoring and

[26] *Supra* 19
[27] *Supra* 15
[28] *Supra* 15.
[29] *Ibid.*
[30] Chapter VIII (Transfer of Personal Data Outside India), The Personal Data Protection Bill, 2018.
[31] *Draft privacy bill and its loophole*, https://www.livemint.com/Opinion/zY8NPWoWWZw8AfI5JQhjmL/Draft-privacy-bill-and-its-loopholes.html (last visited Aug 10,2019).

widespread facial recognition cameras, all connected to integrated data analysis platforms. With the aid of these systems Chinese authorities have, according to the U.S State Department, "arbitrarily detained" between one and two million people.[32]

Suggestions

Algorithms are the foundational blocks of any artificial intelligence-based mechanism. Regulating algorithms therefore enables us to nip problematic reflections of human biasness at the bud and ensure a transparent, just and accountable system. At present there is humungous measure of information available for use and in this way, it might appear to be difficult to keep a check on such data circulation however, the utilization of algorithms in legal, medical, financial and other aspects make it important to have some control instrument set up.

Keeping this in mind different countries have come up with different set of rules and regulations to monitor the usage on algorithmic infrastructure within their territories. Recently, the Algorithmic Accountability Bill 2019[33] was sponsored in the U.S Senate which directs the Federal Trade Commission to require entities that use, store or share personal information to conduct automated decision system impact assessments and data protection impact assessments[34].The overall objective of the act is to directly target potential bias and discrimination in all consumer based businesses and avert any probable harm to the privacy and security of personal data of individuals. The act calls for impact assessment of 'high risk' systems, to evaluate its effect on accuracy, bias, discrimination, privacy etc and check the extent of protection being given to the personal data of individuals.[35]

- An auditing process should be established, in which third party should conduct independent evaluations of these algorithms. Algorithm auditing must be interdisciplinary in order for it to succeed. It should integrate professional scepticism with social science methodology and concepts from such fields as psychology, behavioural economics, human-centred design, and ethics. The problem is that Social Networking became too big to be regulated by a neutral third party or government. It seems that the only option we have is to trust Mark Zuckerberg, Larry page, and Segrey Brin on their good faith and intentions to process and filter information for us. In that situation the criteria given under Algorithmic Accountability Act can be followed which will tackle this problem. The regulations given under this act will apply only to the companies that make over $50 million per year, hold information on at least 1 million people or devices, or primarily act as data brokers that buy and sell consumer data.
- Now that we have made sure that algorithms themselves and the way they are coded there

[32] How Artificial Intelligence Systems Could Threaten Democracy, https://www.govtech.com/products/How-Artificial-Intelligence-Systems-Could-Threaten-Democracy.html (last visited Sept 14,2019).

[34] A look at the proposed Algorithmic Accountability Act of 2019 https://iapp.org/news/a/a-look-at-the-proposed-algorithmic-accountability-act-of-2019/, (lasted visited Sept 10,2019)

[35]Proposed Algorithmic Accountability Act Targets Bias in Artificial Intelligence https://www.jonesday.com/en/insights/2019/06/proposed-algorithmic-accountability-act, (lasted visited Aug 12,2019).

is nothing which perpetuates bias. To ensure that it does not reflect human bias they, the data produced by them should be checked in regular intervals by the companies, similar to internal audit.

- The creation of a grievance redressal mechanism can contribute to implementation of algorithmic infrastructure more efficient. A redressal system will enable the mechanized system to be accountable, responsive and user-friendly. The existing laws give individuals the right to access[36] and erasure[37] but there is an absence of a grievance addressal mechanism. The consumers are not being given an opportunity to given a feedback for their experience and usage of their data by a particular system. For example: When the risk assessment mechanism in the American Criminal System gave the result of black people having more chances of being repeated offenders over white people, there was no system in place for them to be able to challenge the said proclamation. Allowing people to give feedbacks is as important as giving them access for it will not only help increase the efficiency and accountability of the mechanized systems but will also help gain confidence of the consumers and regulate the working of self-learning algorithms by keeping a check on the way they are processing the requisite data.

Algorithms are everywhere and yet the general public has a poor understanding about the sophisticated and insidious mechanisms used by these pre-programmed catastrophes creating system which often results in a blanket assumption that they are neutral in nature[38]thereby underestimating the powerful impact that they have on our lives. In this paper we have analysed the growing effect of algorithmic infrastructure on significant aspects of our lives especially the political bias it causes. We have highlighted features and ambiguities of the existing laws like that of General Data Protection Bill and the Personal Data Protection Bill (draft) and their impact on the mechanized systems. Further, we have given suggestions that can contribute to the creation of a more accountable and efficient algorithmic infrastructure.

*****

[36] See art.15 para 3 of GDPR
[37] See art 17(1) of GDPR