REGULATING ARTIFICIAL INTELLIGENCE (AI) - CASE OF TECHNOPHOBIA?

APRIL 3, 2024

RACHANA RAUTRAY
Anagram Partners

rachana.r@anagrampartners.in

As most countries gear towards regulating AI by adopting either a risk based or use case approach, a fundamental oversight of such regulation has been an overt focus on the results generated by the tool.

This oversight is largely rooted in the surge in popularity of tools such as ChatGPT and Dall-E that seemingly mimic "**human results**". The Indian Government has also fallen prey to 'AI Anxiety' and has had a knee jerk response to regulation through its various advisories, requiring human intervention to a machine learning automation tool. Such regulation has unfortunately failed to appreciate the fundamentals of AI.

What is AI? How is it distinct from other Automation Tools?

Akin to automation, AI has been designed to streamline identified tasks. However, unlike automation that involves repetitive tasks and is programmed to '*perform*' a task, AI is programmed to '*learn to perform*' a task based on, among other things, repetitive tasks. While the basis for automation is software codes, the basis for AI is the data through which the program learns. It is the use of algorithms to process large amounts of data that makes AI unique. Nevertheless, at its core AI is merely an advanced technology tool developed to eliminate human intervention in day-to-day tasks, reduce costs and increase efficiency.

The Indian Journey with AI thus far

Today, India's use and development of AI continues to be in its nascent stage. With India's vast population, the use case for AI is several. Despite this, the Indian Government's approach to AI has been two-fold – on one hand, the Government in its Interim Budget announced a one lakh crore corpus to fund research in advanced technology and is anticipated to roll out another scheme for '*deep tech*' in defense. On the other hand, each of its advisories, until March 15, 2024, highlight the deep distrust with the outputs that AI may generate.

Is there truly a vacuum in India for AI Regulation?

It is the use of large data sets by AI that has attracted global regulatory scrutiny, with concerns ranging from data privacy, copyright infringement, misinformation, defamation, etc. Arguably while these legal issues could equally arise with outputs generated by most technology tools, it is the 'learning' by AI tools and potentially a lack of control by the programmer that has left governments running scared.

If you have any questions regarding the matters discussed in this publication, please contact the attorney(s) listed above or call your regular contact at Anagram.

Data Privacy

In India's case, it is a misnomer to argue that existing legislation does not provide necessary checks and balances to regulate AI. To demonstrate, the recently enacted Digital Personal Data Protection Act, 2023 ("**DPDPA**") has expanded the consent architecture applicable to personal data, wherein any processing of personal data, i.e., collection, storage, indexing, disclosure, etc. of data about an "*individual who is identifiable by or in relation to such data*", would require consent from such individual, except in case of an identified set of circumstances that amounts to legitimate use.

Accordingly, for AI models to be in consonance with Indian law, one would have to demonstrate either that such AI model has been built pursuant to necessary consent being obtained from individuals or through legitimate use. Do note, until the DPDPA comes into effect, the requirement to obtain consent under the (Indian) Information Technology Act, 2000 ("**IT**") only extends to sensitive personal data, i.e., biometric information, financial information such as debit or credit card details, etc. In case of AI, the Government through the proposed rules to the DPDPA would need to throw further clarity on the treatment of data that has been legitimately processed by AI models without consent prior to the commencement of the DPDPA.

In contrast, AI models like '*Devika*'[1] that do not per se process '*personal data*' do not fall under the ambit of the DPDPA. These models continue to understand high-level instructions, reason through complex problems, and generate code in multiple programming languages. To the extent it relies on personal data, developers would have to work towards basing their analysis on anonymized data, such as data sets based on geographies, income classes, or other subsets that average behavioral use, in each case without identifying specific individuals.

Regulating Deepfake

Issues of misinformation on account of manipulation of images or videos, particularly those publicly available, are not unique. Editing tools such as Photoshop, Snapseed, etc. have equally contributed to the spread misinformation, for instance in the 2020 US Presidential Elections. Unlike ordinary editing tools, AI has merely facilitated more '*authentic*' edits that is more tedious to distinguish from original works. However, irrespective of the skill involved in manipulating information, Section 66D, 66E and 67 of the IT Act read with the Indian Penal Code, 1860, attribute liability to the transmission of any images that violate privacy and publish obscene content. Having said this, given the increased spread in misinformation, there is some merit for the Government to revisit the penalties that accrue based on harm caused by misinformation rather than regulating tools that may be used to facilitate such misinformation.

Assigning Liability

In terms of attributing liability, akin to the deployment of technology tools, the test of identifying the data fiduciary, data processor and data principal would have to be undertaken under the DPDPA. Similarly, liability may equally be attributed to the intermediary deploying AI in accordance with the Information Technology (*Intermediary Guidelines and Digital Media Ethics Code*) Rules, 2021 ("**Intermediaries Guidelines**"). To the extent that the platform can demonstrate its due diligence and compliance with the Intermediaries Guidelines, reasons for heightened liability when such misinformation is generated by AI is unfounded.

Are MeitY's Advisories Effective Regulation?

To address issues of reliability in results generated by AI, the Indian Government has pushed liability onto the intermediary to ensure there is no bias or discrimination as well as requires data to be watermarked. For argument, if an intermediary was held liable for biased results and seeks to rely on labelled data sets, it is likely that the dataset itself would not infringe existing laws, but the results would be biased, i.e., a cause of AI hallucination. A classic example is when an AI tool inaccurately identifies healthy blood cells as cancer cells since the datasets that were processed did not sufficiently distinguish between healthy and cancerous blood cells.

Accordingly, merely watermarking various data sets of blood cells would not in itself mitigate or assist with assigning liability for inaccurate results. While platforms may utilize as much data as feasible to train their AI tools, ultimately today there exists no full proof mechanism to restrict all hallucination.

Given the above, there is merit in relying upon existing legislation that sufficiently assigns liability for the use of inaccurate information. For instance, while the Government cannot and does not regulate individual opinions, hate speech or discrimination based on individual opinions may have civil and/or penal consequences.

What Next?

To ensure that India's AI journey does not halt even before its full capability is realized, it is arguable that the Indian Government may need to reassess whether technology specific regulation is necessary to keep pace with innovation. Unlike the EU and US, there is merit to explore other routes to regulation. For instance, Singapore has steered clear of hasty regulation and instead is working with industry professionals to set up necessary framework models to facilitate trust in the use of AI. As next steps, it may be worthwhile to examine whether the possible results of use of AI is sufficiently regulated, or if further clarity to existing legislation is necessary to tackle such results. Ultimately, liability would need to befall the results of such use rather than the deployment or risk of use of a technology tool, akin to existing technology such as search engines or editing tools.

[1] India's open-source project that challenges 'Devin AI' the world's first AI software engineer. Read more here and here.

This publication is for educational and informational purposes only and is not intended and should not be construed as legal advice.

anagrampartners

Mumbai | Delhi

Follow us for more

in / anagrampartners.in

0401—2024