CURRENT SCIENCE

Volume 115 Number 6 25 September 2018

GUEST EDITORIAL

Artificial intelligence policy: Need aggressive development with prudent regulation

Artificial intelligence (AI) is a buzz-phrase these days. Serious computer scientists and researchers have been known to bemoan the fact that their scholarly academic discipline and work are demeaned in the public mind, primarily on account of being conflated with hackneyed software discussions and superficial literature. In similar vein, AI and related topics – machine learning, deep learning, neural networks, etc. – are now to be found embedded in the utterances and writings of a great many people who have neither heard of the frame problem, nor any idea how gradient descent is related to Newton's method.

The reasons are clear: startling uses of AI even in seemingly unrelated fields such as the natural sciences include generating images of galaxies, learning the art of chemical synthesis, finding subtle spatial patterns in particle detectors, or even finding gene variants for autism by studying inheritance patterns in genomes. From finance to agriculture, from security to environment, and from education to healthcare, AI has the power to transform.

Most countries have understood this importance of AI as a technology discipline, and have by now devised significant strategies to deal with its emergence.

In India too, AI is essential for the goals of Digital India to be realized – the huge scope of complex, always available online services for a billion citizens all but rules out 'human in the loop' decision-making (which would be too slow and require too many trained workers). However, India was late to the party – AI in the country has largely a token presence in some multinational companies which have some development centres here. Home-grown efforts on the academic, government, industry and investor fronts are few and far in between.

Furthermore, Indian presence at leading AI research conferences is negligible; academic research in AI is hamstrung by lack of industry involvement, as well as by antediluvian funding policies and inane government restrictions that do not suit the fast pace of AI research.

Perhaps for these reasons, India is way behind China and many other countries in AI. It indeed is behind in related technologies such as high-performance computing, as may be seen from the fact that China is a consistent leader of the top 500 supercomputer list (https://www.top500.org/lists/) – with over 200 entries in that list – whilst India has hardly one or two, near the bottom. We can safely surmise that given current rates and trends, *the gap will not close in our lifetimes*.

Given China's zealous drive in defense-driven AI research (with the stated ambition of being the dominant force in AI by 2030), India could potentially face a near-permanent disadvantage in the balance of power in ways that our strategists and planners can scarcely imagine. Even seasoned Silicon Valley investors have expressed concern at the way the Chinese government is aligned with their tech sector – leading to better funding, less regulatory hurdles, access to larger datasets, and ultimately unquestioned supremacy in AI and related technologies for that country.

In this context, it is imperative that we view AI as a critical element of India's national interests, unlike at present where it receives at most lip service. To address India-specific needs given our unique social context, we also cannot rely on foreign research which will often not suit our priorities and needs; instead the government needs to go all out to foster our own research.

Coming to the global perspective, there is a present-day myth that is often perpetuated, that AI is a fairytale success story – but there have been 'AI winters' in the past when AI fell out of favour, and there might be more to come. AI has its fair share of problems, which may spell grave consequences if left unregulated.

Algorithmic bias and ethics are serious issues, though not as commonly known as they should be. Especially in cases when data points represent real humans, rigorous error analysis becomes supremely important – ML can lead to harm if applied unethically, as algorithms can simply learn and reproduce biases present in datasets used for training. Still worse, many ML algorithms are not explainable, meaning that no one, including the users or even the designers of such algorithms, knows exactly how they produce a particular result.

Hence, AI when applied to social science will pose more challenges than when applied to mainstream computing tasks like theorem proving or chess playing. AI systems must respect socially relevant values. This can be done by the inclusion of ethical principles, which must serve as a true north to every rule. Above all, computer scientists need to work with social scientists to gain deeper insights into how ML models have ethical implications.

Moreover, malicious uses of AI that pose potential threats to digital, physical and social security can impact the design and management of infrastructure. AI can go wrong unintentionally, as in algorithmic bias, but it also carries the potential of deliberate misuse, affecting either specific individuals or even large groups of people. Besides the usual difficulties associated with using hardware and software products, new unresolved complications arise in the wake of AI: these include sophisticated techno-frauds (such as faking a person's voice as making a statement), enhanced quality and frequency of spear phishing (fake online messages sent to gullible victims), data poisoning attacks (creating training data to make an ML system learn erroneous judgments), and others.

Apart from these issues, the recent Cambridge Analytica scandal reminds us that AI in the hands of foreign multinational companies is perhaps a far bigger threat than Aadhaar. The creation of 'data monopolies' by large tech companies – generally American or Chinese – is a big concern, as laymen have hardly any idea what personal data is being collected or how it is being used. The interference in the U.S. presidential elections in 2016 is a wake-up call.

Besides, the diversity of languages and cultures across India is also a challenge for developing AI systems here. A related research priority has to be to develop India-specific models to study the impact of AI technologies on employability, job skilling/training, and wealth generation, while foreseeing how AI may transform Indian society while also affording opportunities to the disadvantaged. Loss of jobs is a problem that is often cited as a disadvantage of AI, but newer ones are also sure to be created – for instance in system maintenance or AI advisory services. Even granting that risk to present-day jobs is real, this only brings up the imperative of re-skilling workers to be employable in AI-driven sectors (such as in the manufacturing industry), and of our educational curricula and training programmes to be upgraded accordingly.

Policymakers in India should keep (domestic) AI at the forefront of the Make in India programme, rather than simply trying to get foreign manufacturers to set up shop in the country. There has to be a deliberate policy to aggressively drive localized AI research and innovation in diverse sectors, while also enforcing prudent regulation that is truly the need of the hour. For instance, in certain social sectors and applications, it is surely inappropriate to permit unexplainable algorithms to be used. A clear framework for transparency and accountability guidelines, and strict national standards and ethical standpoints, need to be established to fight the threat of accidental or malicious bias.

In this regard, the basic structure of a tiered decision-making system – as in other non-digital systems – must be adopted, with auditors who play the role of 'AI guardians'. While humans should always be able to override AI, there arises a question: is any proper bureaucrat at all competent to regulate AI? This means that, for pragmatic regulation, AI researchers need to be involved more than ever in policy-making efforts.

It is pertinent to note here that if India were to actively participate in international AI research and discussions on regulation/rule-making (where it is today almost entirely absent), it would surely help with efforts to bring AI into our society in proper ways.

The Ministry of Commerce and Industry has set up an AI Task Force (https://www.aitf.org.in/) which acknowledges the creation of a policy and legal framework to accelerate deployment of AI technologies across domains as an important goal. It rightly emphasizes that AI should be interpreted as a scalable problem solver, rather than merely a booster of economic growth. The 2018 AITF report provides several ideas like setting up a national AI mission, starting AI talent 'melas', and commissioning six centres of excellence – but there is scant evidence of innovative thinking in the recommendations. Moreover, it is disheartening to notice the poor representation of hands-on AI professionals actually working in industry or academia, in the task force.

Government policies need to be framed with apt collaboration and vigorous discussion with academia, legal institutions, corporate stakeholders, as well as bilateral partnerships. In this regard, we should note that the government think tank NITI Aayog has recently released a discussion paper on AI, with a lot of general information and some specific suggestions (http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf). This is welcome, but it needs to be followed up with suitable further steps. Unless suitable celerity and initiative are shown in the development of domestic AI technologies and prudent regulation of the same, we could well see a dystopian situation soon enough, where on the one hand there is not enough AI in India to serve the proper needs of our society, but there is more than enough to do harm.

Shrisha Rao[1,*]
Deya Chatterjee[2]

[1]International Institute of Information Technology – Bangalore
26/C Electronics City,
Bengaluru 560 100, India
[2]SRM University,
Chennai 603 203, India
*e-mail: shrao@ieee.org