REGULATING ARTIFICIAL INTELLIGENCE IN SOUTH ASIA:

PROJECTIONS FOR THE FUTURE

NUS National University of Singapore | iSAS Institute of South Asian Studies

KONRAD ADENAUER STIFTUNG

About the Institute of South Asian Studies

The Institute of South Asian Studies (ISAS) is dedicated to research on contemporary South Asia.

It was established in July 2004 as an autonomous research institute at the National University of Singapore (NUS). The establishment of ISAS reflects the increasing economic and political importance of South Asia, and the strong historical links between South Asia and Southeast Asia.

The Institute seeks to promote understanding of this vital region of the world, and to communicate knowledge and insights about it to policymakers, the business community, academia and civil society, in Singapore and beyond.

About the Konrad Adenauer Stiftung

The Konrad Adenauer Stiftung (KAS) is a political foundation of the Federal Republic of Germany, which has, for over 50 years, committed itself to the promotion of democracy and international cooperation. Founded in 1964, it was named after the first Chancellor of the Federal Republic of Germany, Konrad Adenauer. KAS offers political and social training activities, conducts research, grants scholarships to students, and supports and encourages international understanding and economic development.

The Rule of Law Programme is a worldwide programme of KAS with regional offices in Asia, Europe, Latin America, Sub-Saharan Africa and Middle East/Northern Africa. The Rule of Law Programme Asia, based in Singapore, is dedicated to working with its Asian partners towards the development of rule of law in the region. It initiated its digitalisation programme to take stock of the regional developments regarding the emergence of new media and advanced technologies. One of the particular areas of focus is to explore the interplay between technology, society and the role of law.

Joint Roundtable by ISAS and KAS
Regulating Artificial Intelligence in South Asia: Projections for the Future
5 August 2019
Authored by Aishwarya Natarajan and Vani Swarupa Murali

Cover design courtesy of Khalsa Printers Pte Ltd

Institute of South Asian Studies
National University of Singapore
29 Heng Mui Keng Terrace
#08-06 (Block B)
Singapore 119620
Tel (65) 6516 4239
Fax (65) 6776 7505
URL www.isas.nus.edu.sg

Konrad Adenauer Stiftung
380 Jalan Besar
#11-01 Arc 380
Singapore 209000
Tel (65) 6603 6171
Fax (65) 6227 8343
URL www.kas.de/en/web/rspa

Regulating Artificial Intelligence in South Asia: Projections for the Future

Institute of South Asian Studies
Konrad Adenauer Stiftung
March 2020 | Singapore

Aishwarya Natarajan
Vani Swarupa Murali

Special Report Issue No. 5

NUS National University of Singapore | ISAS Institute of South Asian Studies

KONRAD ADENAUER STIFTUNG

CONTENTS

Executive Summary

Artificial Intelligence (AI) has the potential to transform the way we live, work and interact. While AI is likely to have a critical impact in key areas such as healthcare, agriculture, education, smart cities and mobility, it also raises fundamental questions about data privacy, mass surveillance and the infringement of fundamental rights.

South Asia faces specific challenges in regulating AI, including the maturity of its legal systems, governance standards and economic development. It is thus important to begin a conversation about whether existing legal and regulatory frameworks in South Asia can effectively foster and regulate the deployment of AI technologies.

The Institute of South Asian Studies at the National University of Singapore and the Konrad Adenauer Stiftung organised a joint roundtable on 'Regulating Artificial Intelligence in South Asia: Projections for the Future' on 5 August 2019. The event brought together researchers, legal and industry experts as well as policymakers to discuss key themes in the AI regulatory space.

This report largely draws upon the discussions at the roundtable. It focuses on two key areas: first, the challenges posed by AI in the fields of human rights, surveillance and data strategies; and second, the imperatives of regulation and how it relates to context and literacy, as well as possible policy recommendations.

The role and influence of AI are likely to continue to grow. However, AI also brings with it certain risks of bias and discrimination that could potentially cause problems.

The role and influence of AI are likely to continue to grow. However, AI also brings with it certain risks of bias and discrimination that could potentially cause problems. For example, since 2017, Aadhaar, India's digital identity scheme, which is also the world's largest, has encountered several problems, such as hindrance to the access to welfare benefits, fingerprint authentication issues and identity fraud. This has resulted in people being denied their legitimate entitlements. Thus, AI brings with it complex challenges, and these challenges necessitate nuanced and sophisticated regulatory mechanisms.

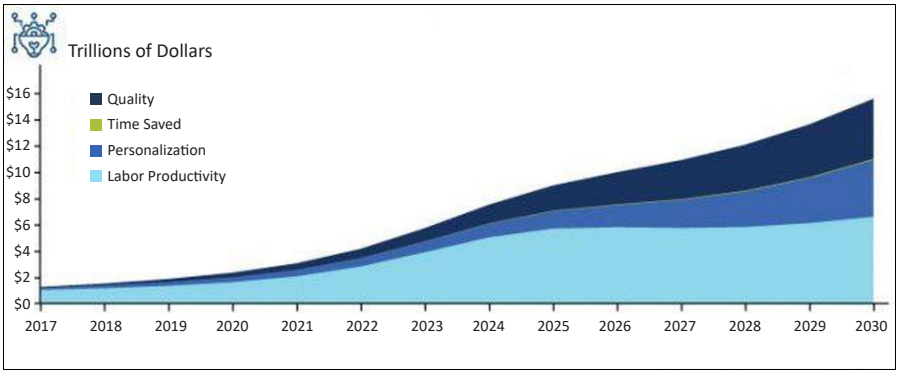
Introduction

AI has been projected to grow rapidly, potentially adding US$15.7 trillion (S$21.9 trillion) to the world economy, which is projected to grow to US$137.5 trillion (S$191.4 trillion) by 2030.[1] This growth in AI's contribution to the economy is up from the US$2 trillion (S$2.8 trillion) that it contributed in 2018 (Figure 1). For comparison, Figure 2 shows the projected gap in growth values with and without the use of AI. As can be seen in Figure 2, AI is predicted to play a vital role in key sectors such as business services, finance, manufacturing, health, transportation, agriculture and public service delivery. This shows the growing importance of AI and the amount of attention that should be paid to its assessment.

AI is predicted to play a vital role in key sectors such as business services, finance, manufacturing, health, transportation, agriculture and public service delivery.

In India, the latest National Institution for Transforming India (NITI Aayog) report states that AI will add US$957 billion (S$1.3 trillion) to the country's economy by 2035. The numbers for AI's projected impact on global growth are also impressive (Figure 3).

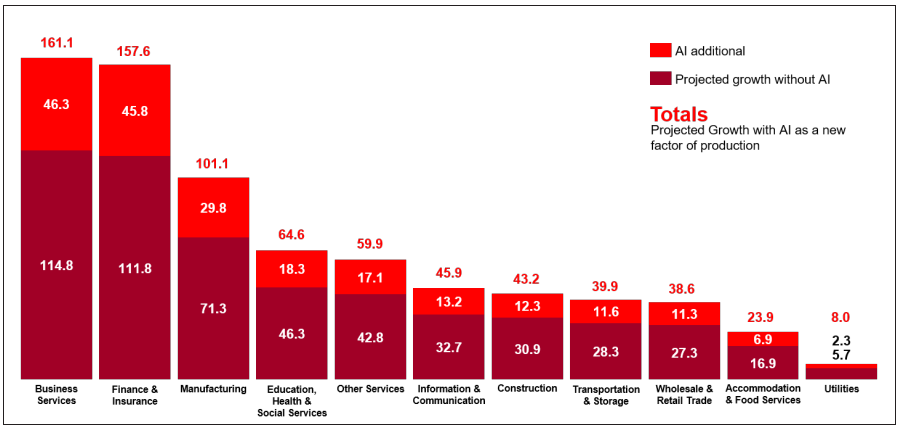
Figure 1: AI's Impact on Global Gross Domestic Product



Source: PwC Global 2019 report 'Sizing the Prize', https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

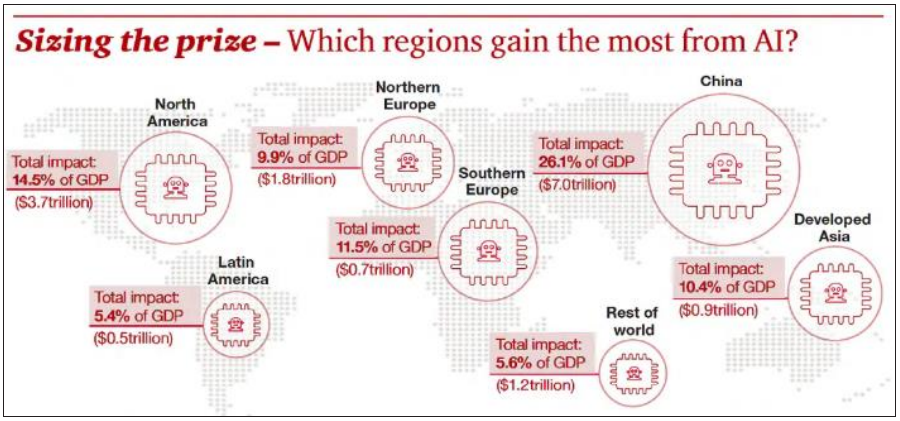
1 OECD Data, Real GDP long-term forecast, https://data.oecd.org/gdp/real-gdp-long-term-forecast.htm#indicator-chart.

Figure 2: Growth with and without AI



Source: Accenture 'How AI Boosts Industry Profits and Innovation', https://www.accenture.com/sg-en/insight-ai-industry-growth

Figure 3: Reach of AI Globally



Source: PwC Global 2019 report 'Sizing the Prize', https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

AI also has agenda-setting and amplifying potential in the way that it can alter public sentiment and opinion.

However, the rise of new technologies, such as AI, has spawned new challenges, such as legal issues, ethical challenges and socioeconomic concerns. AI can potentially subvert democratic processes and institutions. AI also has agenda-setting and amplifying potential in the way that it can alter public sentiment and opinion. As a result, societies that can harness the benefits of AI while also managing its challenges will provide an optimum environment for such technologies to thrive. One of the most widely discussed examples of the risks and rewards of AI is the self-driving car. Programming an autonomous vehicle involves difficult ethical and legal choices that are being debated in several countries.[2]

2 Lat, David, 'The Ethical Implications of Artificial Intelligence', Thomson Reuters, https://abovethelaw.com/law2020/the-ethical-implications-of-artificial-intelligence/.

This would imply that regulation is a necessity and that the debate within the field is more about how to regulate than why. Regulation in this case would be defined as a broad governance framework that includes both legal and non-legal measures such as guidelines. Even within the legal measures, regulation does not refer to a single overarching legislation but several legislations regulating different sector-specific aspects of AI. Looking at it from this point of view would indicate that the need for regulation is commonly agreed upon, but that disagreements arise when looking at specifics and priorities, and when speaking with different actors, groups and regions. Therefore, rather than seeing regulation as a way to restrain technological innovation, there is a need to re-think the way the term is used. Instead, regulation should be formulated in such a way that would enable technology to develop and contribute to human betterment whilst tackling the challenges of digitalisation.

However, there are some who have criticised this view, pointing out that the assumption of AI being inevitable is flawed. The automatic tendency to link AI to a higher level of efficiency needs to be challenged. Instead, it has been argued that such assumptions negate the basic question on whether AI should be used at all. From this perspective, the common question of asking where and how AI can be used fails to answer the fundamental question on what problem is sought to be resolved by its implementation. It is also critical to examine whether the intention behind deploying AI as the solution is to optimise efficiency or social justice or to reduce inequality. It then must be assessed whether AI is the best mechanism to solve that problem.

It is also critical to examine whether the intention behind deploying AI as the solution is to optimise efficiency or social justice or to reduce inequality.

AI cannot have a 'one-size-fits-all' regulation. Implementing a blanket regulation could further complicate the challenges faced. Rather, any regulation should consider the context and the industry. Therefore, policymakers should delve into the nuances of each sector using some level of domain understanding, because each intervention is aimed at solving a specific problem.

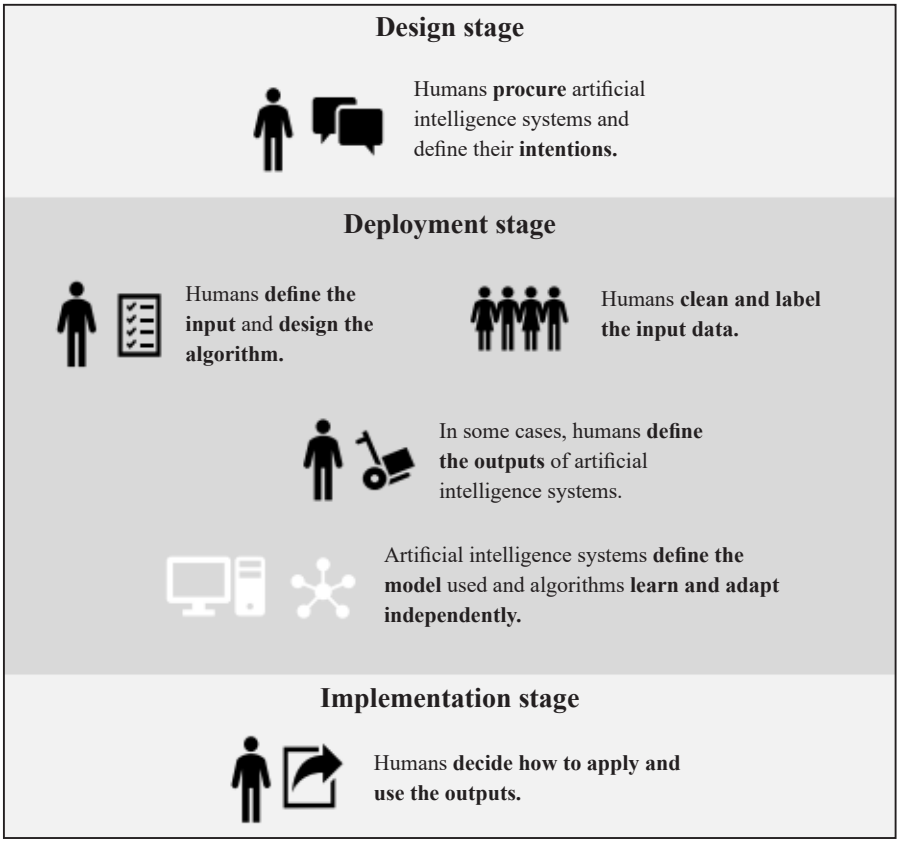
The contents of this report draw largely from the discussions at the roundtable. The report focuses on two main aspects. First, it looks at the challenges faced through the implementation of AI. Second, it touches on the changes in the field of regulation and possible policy ramifications.

Challenges to the Implementation of AI

There is no consensus on the definition of AI. At one level, AI is used to refer to automated computational decision-making. However, a United Nations (UN) report refers to AI as a set of "processes and technologies enabling computers to complement or replace specific tasks otherwise performed by humans, such as making decisions and solving problems". It adds, "AI can be a problematic term, suggesting as it does that machines can operate according to the same concepts and rules of human intelligence. They cannot. AI generally optimises the work of computerised tasks assigned by humans through iterative repetition and attempt."[3]

AI generally optimises the work of computerised tasks assigned by humans through iterative repetition and attempt.

Figure 4: How AI Works



Source: https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ReportGA73.aspx.

3 UN Human Rights Office of the High Commissioner, 'Report of the Special Rapporteur to the General Assembly on AI and its impact on freedom of opinion and expression', 29 August 2019, https://www.ohchr.org/EN/ Issues/FreedomOpinion/Pages/ReportGA73.aspx.

AI systems largely work through the accumulation of data. This reliance on data brings up important issues on the responsible use of data, consent and human rights. Further questions are raised over the kinds of risks that could come up with surveillance to privacy or other aspects of life, such as risks of data theft, misuse, fraud or use of data for discrimination and oppression.

AI has vast potential to be an amplifier. This is problematic when the data that is entered is tainted by current social norms and stereotypes.

AI has vast potential to be an amplifier. This is problematic when the data that is entered is tainted by current social norms and stereotypes. That most of machine learning data is written by men poses a problem. For example, most virtual assistants use a female voice by default. This furthers the gender-biased stereotype that assistants are often women. Again, facial recognition applications are based on predominantly white male datasets, with errors occurring in up to a fifth of the cases involving women and people with darker skin colours. Thus, algorithms replicate and amplify biases in the hiring of women for what are traditionally male-dominated fields.

Challenges to Human Rights

As mentioned earlier, the real world tends to get replicated when it is based on AI, and this could bring up questions of human rights. This is evident in cases such as access to public services. For instance, hospitals can choose to feed their hiring data into an AI algorithm-based system in order to use machine learning and flag good candidates to hire in the hospital. If the machine notices a trend of privileging white male candidates, it will tend to replicate that behaviour. In India, if a dataset includes last names, machines could notice that upper caste last names appear more frequently and end up hiring them more frequently. In this scenario, caste discrimination which is a real-world problem is replicated within the AI system.

In India, if a dataset includes last names, machines could notice that upper caste last names appear more frequently and end up hiring them more frequently.

There are many ways in which the dataset and its structure and collection could exclude populations. For instance, the method of data collection (such as use of biometrics for the Aadhaar system) could exclude marginalised groups like labourers or farmers whose fingerprints might have faded. Such exclusion becomes significant when public service delivery depends on this data.

The UN report notes, "A number of factors ingrain bias into AI systems, increasing their discriminatory potential. These include the way in which AI systems are designed, decisions as to the origin and scope of the datasets on which these systems are trained, societal and cultural biases that developers may build into those datasets, the AI models themselves and the way in which the outputs of the AI model are implemented in practice."[4]

Another aspect is the involuntary renouncing of ownership. For instance, if a person is asked to provide fingerprints for authentication, he/she will be forced to do so even if he/she does not consent to his/her data being collected. Furthermore, technology can often be concealed. For instance, facial recognition sometimes happens at a distance, without the individual knowing that his/her irises are being

4 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations, 29 August 2018, http://undocs.org/A/73/348.

captured. Similarly, visiting a friend's house does not automatically mean consent to an Amazon Alexa[5] listening in to the conversations, transmitting that data, storing it and using it. This raises questions related to consent and ownership in ways we have yet to comprehend.

Given these examples, it is evident that there is often poor access to information, the inability of the underprivileged to deny consent due to low levels of digital literacy and disparate education on the pros and cons of AI, with the underprivileged not receiving much.

5 Virtual assistant developed by Amazon.

Surveillance

Surveillance refers to the monitoring of activities and information such as people movement using closed-circuit televisions or location tracking on mobile phones for the purposes of managing risks or directing policy. Surveillance can be categorised into two types. First, there is state surveillance, which is done for national security and law enforcement reasons. The second is corporate surveillance, or the monitoring of the general public and selling that data for profit.

These two aspects of state and corporate surveillance have desirable and undesirable aspects. From a state surveillance point of view, law enforcement would advance public safety and security. However, the undesirable element would be an Orwellian 'Big Brother'-type environment where citizens are constantly monitored and have little freedom.

At the sub-national level, some technologically advanced states in India, such as Telangana and Andhra Pradesh, have 360-degree profiling institutions of their own. Citizens have raised concerns over how and why this profiling is being conducted. Given that state institutions such as the Department of Statistics are involved in this profiling, many are concerned about living in a heavily regulated and monitored environment.

At the sub-national level, some technologically advanced states in India, such as Telangana and Andhra Pradesh, have 360-degree profiling institutions of their own.

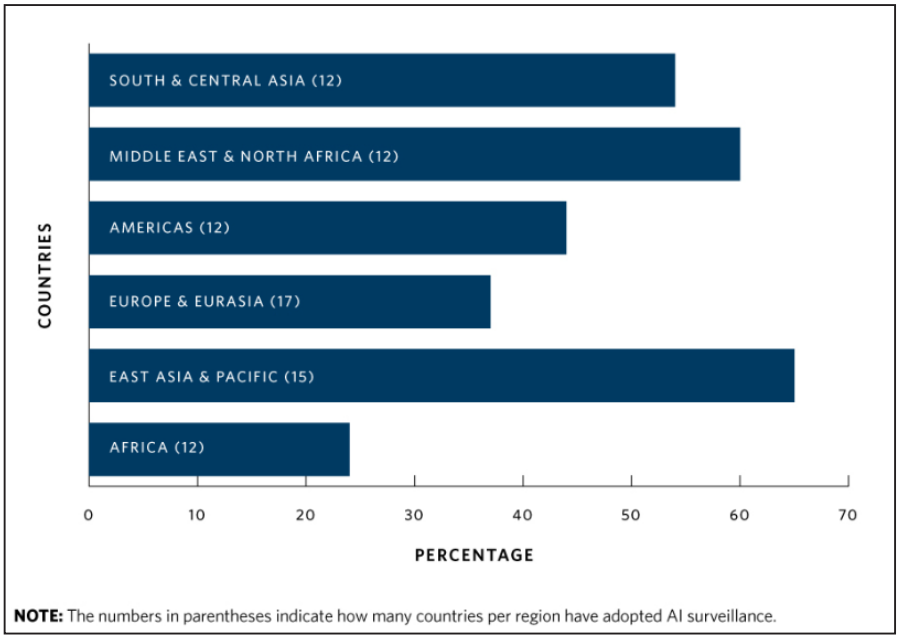
From a corporate surveillance angle, the desirable aspect would be that search engines recommend content based on earlier experiences, which we might enjoy. However, this could also lead to filter bubbles or echo chambers where we only see and consume information that we prefer, and stop receiving information that is contrary to our beliefs.

Surveillance is commonly done through the Internet of Things (IoT), which refers to physical internet-connected devices which can transfer data over networks. The benefit of IoT is that more data can be aggregated to provide better services for people. For instance,

smart traffic lights allow better management of traffic flow or smart water monitors allow monitoring and better control of water usage. Yet, these are potential tools for surveillance, and hackers can steal the data being captured and misuse it. For example, devices such as the smart television or Amazon Alexa are constantly listening in to conversations which can be misused, or smart medical devices could lead to hackers varying medication and causing serious harm to those using the device.

A 2019 report by Carnegie Endowment for International Peace suggests that "at least 75 out of 176 countries globally are actively using AI technologies for surveillance purposes. This includes smart city/safe city, facial recognition systems and smart policing."[6]

Figure 5: Percentage of Countries by Region Adopting AI Surveillance



Source: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

IoT captures behavioural data on people's daily habits, where they shop, who they go out with, at what time they leave home and for how long.

IoT captures behavioural data on people's daily habits, where they shop, who they go out with, at what time they leave home and for how long. Such data cannot be cancelled or erased from the system. As a result, questions arise on what data is being captured, what it is being used for and if decision-making is based on it.

6 Feldstein, Steven, 'The Global Expansion of AI Surveillance', *Carnegie Endowment for International Peace* (2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

An important component that falls within surveillance is privacy. The problem with privacy and consent is that it is not easy to explain the complexity of an AI system and even harder to explain the elements of consent in concealed technology. In such cases, it may not be practical to obtain consent for every sensor collecting data in a particular environment. Because it is not practical, some people are willing to forego their privacy. Their consent to give up their data benefits corporate surveillance through access to vast amounts of data, but such access could lead to dire consequences in the future.

To regulate this, there should be a better understanding of the trade-offs that people are willing to opt for in terms of personal data vis-à-vis functionality. The question of where boundaries lie and to what extent people are willing to give up their data for convenience needs to be filtered back to the AI developers to implement relevant solutions.

The question of where boundaries lie and to what extent people are willing to give up their data for convenience needs to be filtered back to the AI developers to implement relevant solutions.

As a result, activists have pushed for regulation on state and corporate surveillance on data collection and data protection. A crucial aspect of this lies in the formulation of the data strategy, further elaborated in the next section.

Data Strategy

Data strategy is largely formulated by understanding concepts of data ownership, what purposes the data can be used for, how long one has access to the data and whether the data is being used most efficiently for that context.

The case study revealed that the problem was not with the system being designed wrongly but that it was grounded on biased data.

Using the case study of Google's search engine, the issue of gender-biased data was raised. Google, which captures a lot of our day-to-day data, such as gender, designation, etc., found that despite similar designations and work experience, men and women were recommended different levels of jobs by its search engine. In this case, men were recommended higher level jobs while women were recommended lower level jobs. The case study revealed that the problem was not with the system being designed wrongly but that it was grounded on biased data. This was because the data that the system was trained on included significant data where women were either not earning or earning relatively less than men. As a result, predictions for job recommendations were also biased.

Similarly, Google Translate also produces incorrect translations because of gender-biased data. For instance, a trial was conducted converting English to a genderless language, such as Turkish, where genders are represented with the same letter. In this case, the phrase 'he is a housewife and she is a scientist', when translated from English to Turkish and back to English, becomes 'she is a housewife and he is a scientist'. Again, the trial revealed that the problem was not with the technology but on the kinds of data that it was using and the nature of its inputs.

This is one aspect of data regulation strategy that poses a challenge to the AI ecosystem. Since AI evolves quickly with newer data, it needs to be fed unbiased data as inputs.

The second aspect is related to sensors that collect vast amounts of data and pool it. This causes a security problem, because there are

many such sensors that store data in a centralised system. This also means that, because these sensors are receiving data almost every second, there is plenty of irrelevant data in the system. Without any regulation or protection, this would lead to a centralised cloud provider holding on to a vast amount of data, making it a potential target.

The potential risk from a data-rich centralised system is that an attacker can flood the centralised system with irrelevant data. This could lead to a vendor lock-in, where the cost of switching to a different vendor is so high that the customer is essentially stuck with the original data provider.

The potential risk from a data-rich centralised system is that an attacker can flood the centralised system with irrelevant data.

Regulation of AI

It is important to look at AI regulation not as imposing boundaries, constraining its development or retarding progress. Rather, we should take on a more balanced view and see how regulation promotes technological innovation with minimal disruption and harm. It is thus important to see how trade-offs can be reconciled in a way that industry, governments and AI users can reach a mutually compatible outcome which ensures safety and rights for everyone.

It is also important to take several steps back and make sure that the entire AI ecosystem is more inclusive – from technology professionals and business heads to policy designers.

As seen earlier, AI has the potential to negatively affect society, and this is a consequence of the 'pipeline problem'. The pipeline problem is the need to regulate the entire chain of processes from data aggregation to AI deployment. However, just addressing the symptoms that arise from the pipeline problem is not enough. It is also important to take several steps back and make sure that the entire AI ecosystem is more inclusive – from technology professionals and business heads to policy designers.

Starting from the foundation of the AI pipeline, which is data aggregation, the first thing to look at is whether the data that systems are being developed on are biased. The examples discussed earlier emphasise the importance of finding ways to debias or clean data.

In the training phase, it is important to regulate what the AI prototype models learn and what they can infer. After the models aggregate the data, they make inferences from the data.

After deploying the model, there is a need to ensure that the model is not learning biases from external sources, such as user feedback in automated chatbots. In the case of a live model, there is a need to keep feeding more data to the model so that it does not become outdated. It is important to note that even if the data and model are unbiased during deployment, it does not guarantee that the model will be unbiased in future. Constantly checking at the retraining or maintenance phase could help to regulate the system so that it does not contain any biases or learn any new biases.

Through these three phases, the entire pipeline can be checked and regulated to be bias free. Although the regulation of the model is important, other problems also need to be regulated. For instance, in Singapore, the pricing of utilities is regulated by government bodies, but who will regulate the price of AI development? Will the government subsidise the development and deployment of AI? Who will regulate the price of non-governmental development of AI? These are also other questions that need to be asked.

Context

Context plays a crucial role in AI regulation. It is important for governments to come up with an appropriate data regulation strategy for each setting based on their own individual background.

In the developing world, there has been an urge to leapfrog various stages of development. However, whilst AI could provide solutions in sectors such as healthcare, it could also be a less than optimal solution exacerbating existing inequalities or problems in others.

The institutional safeguards that exist in developed countries, such as the General Data Protection Regulation (GDPR), do not exist in many developing countries.

The institutional safeguards that exist in developed countries, such as the General Data Protection Regulation (GDPR), do not exist in many developing countries. This means that the developed countries have an entire system designed around the idea that citizens have an actionable right to privacy. However, when the social media algorithm is moved to a developing country where these safeguards do not exist or are not as stringently enforced, serious challenges arise. For instance, Facebook assumed that there would be a functional media ecosystem in Myanmar, where people would be able to crosscheck the information seen on Facebook with other sources. However, Myanmar did not have such an ecosystem. As a result, Facebook unintentionally ended up stirring divisions. This example reflects the importance of context and the way policy designers (technology, industry or government) should take into account the various contexts that they seek to implement their policies in.

A positive example of context is Sri Lanka. The country aims to have an AI policy covering education, government, agriculture and health by 2020. However, the country did not have any laws on data protection and privacy until recently. Yet, the process by which it has been drafting their laws has been very inclusive. The government engaged a wide range of stakeholders from the telecommunications, financial, manufacturing and other information technology (IT) and non-IT sectors. Whilst it drew largely from the GDPR principles through such engagement, it tailored its policies to the local Sri Lankan context.

Literacy

Digital literacy is also very context dependent. It is defined as having the skills one needs to live and work in a society where communication and access to information is increasingly through digital technologies like internet platforms, social media and mobile devices. It has also been proven that older populations use the Internet significantly less than younger people. Digital literacy does not refer merely to obtaining consent. Rather, it is more about people knowing and understanding what they are consenting to. The process for securing consent has to be more nuanced and comprehensive, depending on the end use of the data. For example, in clinical trials, consent forms must be read out and participants have to understand and repeat it back with a witness present while the whole process is being recorded on video and stored. Given the low levels of digital literacy in Asia, a model based on a simple check in user consent may not strengthen data privacy. The idea of a meaningful informed consent is a myth, given that the large social media platforms are largely owned by the same corporations. Thus, there is a serious need to consider alternate forms of consent to strengthen data protection.

Digital literacy does not refer merely to obtaining consent. Rather, it is more about people knowing and understanding what they are consenting to.

Educating people better about social media use would be a more feasible solution than trying to control information flows from one person to the next. This would have proved an effective strategy to prevent the mob lynching in India fuelled by WhatsApp rumours between 2017 and 2018. In the case of the mob lynching, the most effective measures were those taken by the local police, who reached out to the communities which had no police access. They also helped quell the latter's fears about the messages being real. At the same time, the police's action helped convince the people that the messages being spread were false. Rather than the government blaming WhatsApp, the more feasible and effective approach is to identify the root of the problem, which is the failure of digital literacy.

In the deployment of AI, there has been a lack of basic knowledge and understanding amongst developers about the risk factors associated

In order to address AI regulation, it is important for all users and stakeholders to have a clear idea on the technology and its value to the economy.

with it. Many developers are unaware of the manner in which AI is being used to address potential misuse of data by AI systems. For instance, special attention needs to be paid to add new content into the education systems for students, policymakers, users or even those with no accessibility to digital platforms about digital literacy and its impact on society. In order to address AI regulation, it is important for all users and stakeholders to have a clear idea on the technology and its value to the economy.

There is also a need to get technological practitioners to speak to sociologists and other social scientists so that there is mutual understanding of how the different spheres work.

Those with the least resources and the most vulnerable are somehow given an additional responsibility of becoming digitally literate, with minimal support from institutions. At present, digital literacy is centred on urban centres in South Asia. Given that many are not equipped with digital literacy, there needs to be a more bottom-up approach by the government in addressing the issue.

With literacy, people should be more responsible in how they use the AI systems. For instance, when people understand their rights with laws and regulations, they would react in a more constructive manner by providing feedback to legislators about whether the law needs to be updated over time. This mindset and awareness would prove useful in the implementation of any regulation, and would require a minimal level of civic awareness and digital literacy.

For rural India, which fares lower in terms of digital literacy levels, this awareness of data usage needs to be created by law. This should be done in order to educate people on what is being collected on their behalf and how it is being used. This information should also be proactively disseminated through flyers and posters rather than provided on request. The government needs to be more active in helping the less digitally literate in their decision-making process.

Policy Recommendations

Based on the earlier challenges, there is a need to create a more conducive political, economic and legal environment that can accelerate AI adoption. It is important to assess the application of AI in terms of what it can do for the public good. AI has immense potential to transform society. For instance, about 60,000 children go missing in India every year. However, once the Delhi government put AI solutions into place they could identify 3,000 missing children within a month of their disappearance.

AI has immense potential to transform society. For instance, about 60,000 children go missing in India every year.

Another positive example would be the use of patterns to predict cyclones in advance or Google translate to help cross-border interactions. These examples highlight the positive effects of AI technology. However, there is a fine line between these tools being beneficial and becoming harmful. Regulation should focus on the latter. There is a part of machine learning which is used for beneficial purposes but that could also slip into becoming harmful. For instance, removing personal discretion from bank loan approvals would be an exercise that is handed over to machine learning. Instead of looking at faces or names, machine learning will solely assess based on credit history. Whilst this seems like a beneficial process, the input of biased data could fuel discrimination instead.

AI is unpredictable in the way it could react when coming into contact with messy real-world situations, where people have implicit biases. Therefore, one recommendation to help reduce the possible challenges of AI deployment is to start with a small-scale pilot, where personal data is not involved. This could perhaps be meteorological or agricultural data where no sensitive personal data is required and for which the system can be trained. This system could then be extrapolated to small pilots in other contexts. This would be useful especially in terms of public service delivery. Starting the use of AI to decide personal benefits, welfare entitlements or access to schemes could expose people to real indignities and harm, especially if the systems are not transparent or cross-examined. Until this pilot reaches

a stage of maturity that meets a certain criteria, the model or system should not be allowed to be deployed in other contexts.

Due to the issues around regulation, one of the questions raised is about standard setting. A key question is whether there should be universal standards for AI development and deployment.

Due to the issues around regulation, one of the questions raised is about standard setting. A key question is whether there should be universal standards for AI development and deployment. However, on issues of privacy, surveillance, data management and ethics, some countries may adhere to one set of standards while others adhere to different standards. Alternatively, the onus could also fall on the private sector to lead the process of regulation by normalising certain 'best practices'. This could become so common that the law eventually recognises it as the standard to follow. For instance, industry standard-setting bodies such as the International Organization for Standardization and the British Standards Institution set the framework, and these eventually became legal requirements to comply with. This shows that industry regulations could be picked up by the government to lay down procedures that would have to be complied with to release or use a particular technology.

This process could become more seamless by having specific committees set up to look at policy from a governmental point of view and from an IT stakeholder standpoint. A clear communication line between these two parties could help create a successful regulation that is relevant and useful to all. A successful example of this is evident from Sri Lanka's construction of its national strategy on AI. This process involves state and non-state actors and is led by the Sri Lanka Association of Software and Services Companies. They have currently outlined three key principles: transparency through constant engagement of the private sector, civil society, international partners and government; prioritisation of the broader national vision, rather than looking at one sector or agency more than the other; and practicality, by starting with solutions that reap benefits for the population in the short and medium term.

To ensure that algorithms are built right, another recommendation is that of model certification. For instance, there are many digital

agricultural companies which work on sowing advisories. These companies guide farmers on when they should sow their seeds by looking at various parameters, such as weather or crop patterns, moisture content in the soil, etc. The problem arises when the companies get their predictions wrong, as this could lead to a complete crop failure. In this scenario of not knowing who should take on the responsibility – the digital agricultural companies or their AI model – it would be useful for the companies to certify that it was tested according to all parameters and was safe for public transmission. Therefore, one of the recommendations is to apply this model certification for every AI model that is being deployed in a public setting. However, the issue of who would certify these models, and what metrics to be used, is a moot point.

A possible solution to this problem is to have specialised regulators at various levels of government. For instance, the telecommunication regulating authority and the insurance regulators could be at a national level, the transport department could handle autonomous vehicle regulations at a state level and the municipal level could gather data to understand water consumption levels to provide for water and electricity. It is recommended that instead of a top-down law governing machine learning, this level of detail is necessary for each agency and sector. Laws would not be defined by just one entity, but rather by consultation amongst all the relevant departments.

Alternatively, there could also be an independent oversight committee or officer who functions in complete independence and assesses technological development and the use of AI. This individual or body could examine the level of transparency and compliance with cross-border regulations.

Alternatively, there could also be an independent oversight committee or officer who functions in complete independence and assesses technological development and the use of AI.

We should also consider signalling. In order to know when AI is used, it is recommended having a signal or icon that would indicate when a decision is made purely through automation. This would flag whether a decision is made using human discretion or if it was purely automated. If the latter, there should also be an accompanying option to have an

alternate second opinion using human discretion. The signal could be in the form of a tag on datasets where the distribution of data and the percentage possibility of a biased dataset are indicated.

Legal Recommendations

Beyond the issue of whether there should be a law to regulate the industry, questions also emerge on what kind of law should be drafted and the ways in which it could be implemented.

The challenges that come out of creating a legal framework bring up other issues, such as liability and negligence. On liability, the question is who would bear the responsibility if AI gets its prediction wrong. The challenge is that there are many stakeholders who are involved in running the AI system (author, programmer, developer, owner, etc.). From a criminal liability standpoint, issues of *actus reus* and *mens rea* (the principle of being able to prove that the perpetrator committed the deed and had intended to do so) come into play. For instance, one could factually demonstrate that AI made the mistake, but it would be difficult to prove that the AI system had the intent to do so.

The challenges that come out of creating a legal framework bring up other issues, such as liability and negligence.

There are also issues of tort law and negligence principles that come up when constructing a legal framework. In this respect, questions such as whether one can impose a duty of care on an AI system (and if so, who one would impose the duty of care on), whether the duty has been breached, or if there are damages that flow from the breach, etc., are relevant. These factual questions also bring up the principles of explainability and evidential challenges when prosecuting or investigating an AI system. The current model functions such that developers expect the AI systems to learn and iteratively improve. This means that the application of legal parameters and constraints should also be in a constant state of evolution. Therefore, for a successful implementation of any AI policy, regulation would need to be looked at in a very iterative, consultative and inclusive manner, involving both the legal and technological stakeholders in a constant conversation on the impact of AI on society and those with the most potential to be affected.

There should also be a distinction between the data owner and regulator. In order to regulate this field, the entity responsible will

be based on the definition set by the state for the actor, designer, user and beneficiary. There also needs to be decision support systems with key performance indicators and benchmarks to identify who is responsible for which purpose and which decision.

Appendix 1
List of Participants

Moderators

Associate Professor Eugene TAN
Associate Professor of Law
Singapore Management University

Mr Rajesh SREENIVASAN
Head, Technology, Media and Telecommunications; and Director
Rajah & Tann Technologies Pte Ltd
Singapore

Mr Benjamin ANG
Senior Fellow, Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University

Ms TEO Yi-Ling
Senior Fellow, Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University

Speakers

Professor C Raja Mohan
Director, Institute of South Asian Studies
National University of Singapore

Ms Gisela ELSNER
Director
Rule of Law Programme Asia
Konrad Adenauer Stiftung, Singapore

Dr Ronojoy SEN
Senior Research Fellow and
Research Lead (Politics, Society and Governance)
Institute of South Asian Studies
National University of Singapore

Participants

Ms Chinmayi ARUN
Assistant Professor of Law
National Law University
New Delhi, India

Mr Rushikumar BHATT
Head of Artificial Intelligence
LinkedIn
Bangalore, India

Dr Diganta DAS
Assistant Professor
Humanities and Social Studies Education
National Institute of Education
Singapore

Mr Waruna Sri DHANAPALA
Senior Assistant Secretary
Ministry of Digital Infrastructure and Information Technology
Government of Sri Lanka

Mr Mohammad Arfe ELAHI
Chief Technology Officer
a2i Program, ICT Division
Bangladesh

Mr Faruq FAISEL
Regional Director
ARTICLE 19 Bangladesh & South Asia

Ms Malavika JAYARAM
Executive Director
Digital Asia Hub
Hong Kong

Ms Nishtha MADAAN
Research Scientist
IBM Research AI
India

Ms Aishwarya NATARAJAN
Research Associate
Rule of Law Programme Asia
Konrad Adenauer Stiftung, Singapore

Mr Mohanakrishnan P
Head, Centre of Excellence
Data Science and Artificial Intelligence
NASSCOM, India

Mr Alok PRASANNA
Senior Resident Fellow
Vidhi Centre for Legal Policy
Karnataka, India

Mr Yudhanjaya WIJERATNE
Researcher
LIRNEasia
Sri Lanka

Appendix 2
About the Authors

Ms Aishwarya Natarajan is a Research Associate with Konrad Adenauer Stiftung's (KAS) Rule of Law Programme Asia, where she is the lead researcher tracking legal policy developments in Asia. One of her core research interest at the foundation is to look at the growth of advanced technologies and its implication of the existing legal frameworks in Asia specifically in the areas of constitutional law, ethics and human rights.

Ms Natarajan is a lawyer by training and practiced as a corporate lawyer with leading law firms in India. Prior to joining KAS, she worked with the Law Society of Singapore on law reform matters and use of technology in legal sector.

She holds an LLM in Corporate and Financial Services Law from the Faculty of Law in the National University of Singapore and an MSc in International Relations from the S. Rajaratanam School of International Studies in Nanyang Technological University.

Ms Vani Swarupa Murali is a Research Analyst at the Institute of South Asian Studies in the National University of Singapore. She completed her Masters in Asian Studies at the S. Rajaratnam School of International Studies in Nanyang Technological University. She has a Bachelor's in Social Sciences from the Singapore Management University.

Ms Murali's research interests are domestic politics and rural development in India. Specifically, she looks into India's agrarian distress and farmer rights.

Institute of South Asian Studies
National University of Singapore
29 Heng Mui Keng Terrace
#08-06 (Block B)
Singapore 119620
Tel (65) 6516 4239
Fax (65) 6776 7505
URL www.isas.nus.edu.sg

Konrad Adenauer Stiftung
380 Jalan Besar
#11-01 Arc 380
Singapore 209000
Tel (65) 6603 6171
Fax (65) 6227 8343
URL www.kas.de/en/web/rspa