Infosys cobalt

VIEW POINT

NAVIGATING THROUGH THE EMERGING AI REGULATORY LANDSCAPE – A SECURITY AND PRIVACY PERSPECTIVE

Abstract

It has been 90 years since Alan Turing sowed the seeds of AI. It continues to evolve (especially with the advent of Generative AI), with significant impact to the lives of millions of people (and many businesses) worldwide, potentially bringing in a paradigm shift and transformation. As with any technology advancement or unbridled innovation, AI too has potential negative impact if falling in the wrong hands or applied in inappropriate ways. This has triggered discussions and debates across the world (with varying levels of focus and progress) on bringing in systemic/process controls on AI and guided/governed through regulations and frameworks, so as to balance between innovation and the society at large.

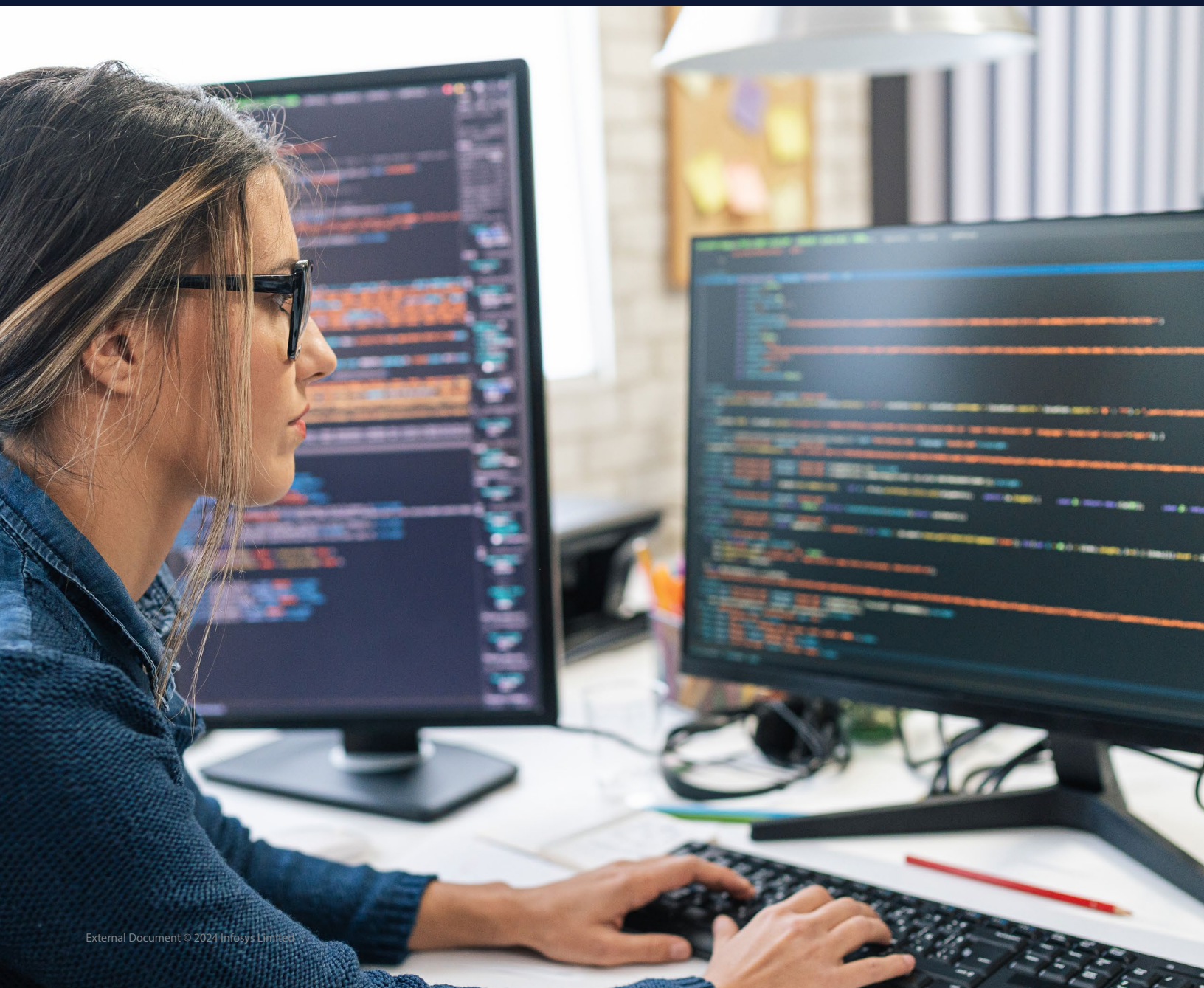
Infosys®
Navigate your next

Introduction

The Industrial Revolution in the 18th and 19th century was a turning point in human history, not only transforming industrial production but also changing the standard of living for majority of the world's population. This had a cascading effect and areas like housing, education and technology advancements flourished, aided by a financial ecosystem to meet the needs of the growing economies. This had its downsides too and resulted in the first known introduction of regulations by governments to bring in some structure, predictability, and accountability in protecting the people and the economy. And this also had (in its nascent stage) elements of what we term as ESG now.

Since then, the world has seen numerous waves of transformation over centuries - advent of the internet and WWW in the late 1960's, and in recent decades the *digital transformation* journey through RPA, SMAC, and AI/ML - accelerated by the more recent pandemic. Governments and regulators across the globe have tread a fine balance on holistic stakeholder value proposition in managing these disruptive changes, having faced with clamors from two divergent schools of thought - restricted usage and regulations on the new technologies and ways of working focusing on protecting human rights and broader stakeholder interests on one side Vs market driven and self-regulated business models where the focus is more on the ease of doing business, enhanced profitability and propelling growth.

It is in this backdrop that we must look at the enhanced focus on regulations for four of the (relatively) emerging and interrelated domains (all of which have in common a critical success factor viz. trust of the stakeholders) – security, privacy, ESG and AI. While the first three have made fairly good progress over the years with increased stakeholder collaboration and concurrence, for AI it's in relatively early stages, though it has been close to 90 years since Alan Turing sow the seeds of AI.



The emergence of AI and the after-effects

While AI powered systems and processes have been aiding in informed decision making in various sectors, there has been concerns over the ethics, privacy, high potential for abuses/ failures (especially related to biased algorithms, social engineering, phishing, malicious code injection, AI hallucinations, copyright infringement, deepfakes, and other synthetic content with potential to influence public opinion or risk public safety).

As AI gets extensively leveraged in domains like Healthcare, the success of AI models (and improvements in algorithms towards that) depends largely on the quality, size and spread of the datasets. With AI systems relying on chatbots gathering personal data across various sources, and broadcast them including to undesirable audiences, data privacy concerns have increased.

The recent advances in Generative AI (expected to grow to 200 BUSD market size by 2032) have accelerated this debate around the importance of addressing related ethical and privacy/security concerns, and has led to increased investments.

The relevance of AI (as well as related risks) is getting much more pronounced with avenues of convergence of AI with Cloud evolving in big data analytics and many other use cases. These offer tremendous opportunities for businesses of all types and sizes to accelerate their digital transformation initiatives. Similar is the potential for blockchain and IoT as well. A recent study by AWS said MSMEs in the healthcare, education, and agriculture sectors will be able to unlock up to 161 Billion USD in annual productivity gains and support 95.8 Million jobs by 2030, equivalent to 8 percent of the total employment on average across the 12 countries studied. This wave of digital innovation and productivity enhancement will be driven by a new range of technologies such as AI/ML and expected to continue as cloud adoption and the AI technology continues to advance.

Also, Generative AI expands the attack surface and exposes new attack vectors to hackers, thus helping them with innovative approaches deceiving conventional security measures and leading to increased financial/reputational risks. This is reflected in a recent Salesforce survey, where 71% of 500 senior IT leaders opine that Generative AI is likely to introduce new security risks to data.

This necessitates close attention to good practices in data privacy and data management, in line with the ethics/values and processes/governance around business and security. Following a risk-based approach, this is often achieved through a combination of techniques including awareness training, anonymization, transparency, aggregation, data minimization, purpose limitation, strict role-based access controls, and validating these and ensuring lawful processing for third party data sources – and have standards, guidelines, and regulations to define the norms and benchmark against those.

As Avivah Litan, Gartner Distinguished VP Analyst says, *"Organizations that do not consistently manage AI risks are exponentially more inclined to experience adverse outcomes, such as project failures and breaches. Inaccurate, unethical, or unintended AI outcomes, process errors and interference from malicious actors can result in security failures, financial and reputational loss or liability, and social harm. AI mis-performance can also lead to suboptimal business decisions."*

AI regulations across the world

In terms of AI related regulations, with the AI legislation journey starting in 2016, around 127 countries currently have laws related to AI, and the recent years have seen an increased focus from the perspectives of security and privacy, thus being treated as inter-disciplinary. Further, nearly 6.5 times increase has been observed on references to AI in global legislature records of 81 countries during this period. If we look at the citizens' acceptability of benefits from AI, figures from Asia and the Middle East are seen significantly higher as against North America.

With AI making inroads into every sphere of people's lives, lawmakers and regulators (in collaboration with industry) are working to regulate the technology appreciating its full range of potential effects — both the benefits and the harms. However, countries have taken differing approaches to AI, in line with their respective legal systems, cultures and traditions.

Generative AI chatbots have been leveraging large language models trained on diverse data sets including from the internet (which has the risk of being exposed in data breaches and has practical challenges to exercise individual "right to be forgotten"). The approach to regulate this varies across jurisdictions – while the US privacy laws like CCPA and CPRA currently do provide some flexibility to businesses on this (though there have been FTC decisions to destroy algorithms trained on unlawfully collected personal data), their EU counterpart (GDPR) insists on a legal basis for handling public data.

Below is an overview of the key AI strategies and regulations across the globe:

- **EU** - On 11 May 2023, European Parliament voted in favor of adopting the EU Artificial Intelligence Act, which in its current form, bans or limits specific high-risk applications of AI. The law is now under trilogue negotiations between Parliament, the European Commission and the Council of the European Union, with a provisional agreement reached on 8th December, 2023.

Keeping in mind the risks (especially to human/privacy rights) emanating from unbridled innovation in AI, the EU AI act has been proposed as a comprehensive legislation in the EU (and the world's first), in line with the spirit of GDPR, setting a global benchmark.

The act aims at establishing a regulatory framework for AI that ensures the technology is developed and used in a way that is safe, transparent and respects fundamental rights – with focus on data quality, transparency, human oversight, accountability, ethical questions, and implementation challenges.

While applicable to a wide range of industries, it is more relevant to those using high-risk AI systems (such as healthcare, transportation, energy, and public safety).

When enforced, the steep non-compliance penalties – even for providing false or misleading documentation to regulators, and up to the higher of €30 million or 6% of global income - is expected to be an effective deterrent.

The EU-wide application of the law is expected to be overseen by a proposed AI Board. Whereas the approach for individual member states need to evolve – there are two schools of thought (with its pros and cons) being considered viz. a single central agency in each member state vs freedom to member states to establish multiple market surveillance authorities as they deem fit.

Looking at the history of GDPR and the complexity of EU decision making process, the legislation may take a while to conclude with a balanced (and scalable) view across all stakeholders.

The Act follows a risk based approach, where systems are classified into 4 levels of risk – 1) Low risk systems 2) Limited or minimal risk systems 3) High-risk systems (including biometrics, critical infrastructure, essential public services, law enforcement, border control etc) and 4) Systems with unacceptable risk (including manipulative or exploitive techniques causing harm, real-time biometric monitoring used in public areas for law enforcement, all forms of Social Scoring etc).

- **UK** – On similar lines as the approach in UK GDPR, UK is working on a strategy providing a framework for identifying and addressing risks presented by AI while taking a balanced approach which is *proportionate* and *pro-innovation*. The UK view is that its established online platform and digital services regulators (like Ofcom, ICO, CMA and FCA) are equipped to head off risks posed by AI systems, through the existing laws and regulations.

- **US** - While there have been global developments in AI law and policymaking, there has been traction in the US as well. A series of AI-related initiatives, laws and policies have been put forth by various government wings and agencies – including The White House, Department of Justice, Congress, FTC, the Consumer Financial Protection Bureau, Equal Employment Opportunity Commission and the NIST.

The FTC announced its plans to soon increase its scrutiny on businesses that use AI. They had earlier warned businesses to avoid unfair or misleading practices, and clarified that in addition to the FTC Act, civil rights laws, torts, and product liability laws also apply to AI.

The CFPB issued a circular requiring creditors using algorithms to provide specific reasons for adverse credit decisions.

The DOJ's Civil Rights Division clarified that the Fair Housing Act applies to algorithm-based tenant screening services.

The EEOC published a technical assistance document describing the applicability of the Americans with Disabilities Act to automated decision-making in the employment context.

The FDA has also announced its intention to regulate many AI-powered clinical decision support tools.

The foundation of the federal government's AI strategy is in place and provides insights into how the legal and policy questions brought about by AI will be addressed, albeit following an ad-hoc or use-case specific approach. Though various city and state AI laws came into effect over the years, and there have been voluntary actions by few technology companies, a comprehensive legislation in the lines of the EU AI Act is expected to take more time to complete the whole cycle of deliberations across stakeholders including businesses and legislators.

- **Canada** - The proposed Artificial Intelligence and Data Act is part of a broader update to the country's information privacy laws and is one of the three pieces of legislation that comprise Bill C-27, which passed its second reading in the House of Commons in April 2023. Towards mitigating harm and biased outputs by AI systems, the AIDA includes a formidable enforcement mechanism. While initial focus will be on guidelines towards compliance through voluntary measures, there is a governance structure being planned through a AI and Data Commissioner working along with the Minister of Innovation, Science and Industry – with empowerment to impose injunctions and penalties as needed. This covers unlawful possession of data for use in Ai systems, systems causing serious harm (with or without intent to commit fraud or cause loss). The expectations are also expected to be proportionate to the size of the organization to ensure operational convenience for new businesses.

- **China** – In Early 2023, the Cyberspace Administration of China released its draft Administrative Measures for Generative Artificial Intelligence Services, towards ensuring content created by generative AI is consistent with "social order and societal morals," avoids discrimination, is accurate and respects intellectual property. There is reference to enforcement mechanisms, though the mechanisms themselves are a web of overlapping authorities, and referenced to cyber and data security laws, as opposed to the AI regulations themselves. Therefore, the AI-specific legislation needs to be looked at within the context of China's wider information privacy and cybersecurity landscape.

- **Singapore** - Singapore's National AI Strategy, meanwhile, consists of the 2019 launch of its Model AI Governance Framework, along with Implementation and Self-Assessment Guide. The aim is to fundamentally rethink business models, to make impactful changes to reap productivity gains and create new growth areas. By 2030, through an ecosystem of enablers for AI innovation and adoption, Singapore is poised to transform itself to be a leader in developing and deploying scalable, impactful AI solutions that can deliver strong social and economic impact, in key sectors (like Healthcare, Smart estates, Education, Border security, Logistics, Finance and Government) of high value and relevance to citizens and businesses.

NIST AI Risk Management Framework (AI RMF)

In collaboration with the private and public sectors, NIST has developed a framework to better manage risks to individuals, organizations, and society associated with AI. The NIST AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.

Released on January 26, 2023, the NIST AI RMF was developed through a consensus-driven, open, transparent, and collaborative iterative process. It is intended to build on, align with, and support AI risk management efforts by others.

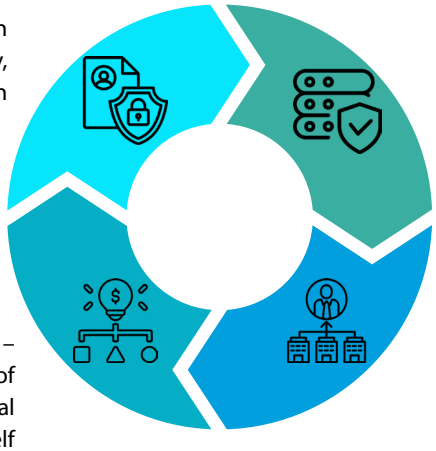
On March 30, NIST launched the Trustworthy and Responsible AI Resource Center, which will facilitate implementation of, and international alignment with, the AI RMF.

How should organizations prepare to be compliant with AI regulations?

AI regulatory enforcement is being approached differently across jurisdictions. However organizations will be better placed on compliance front, through the following :

Exposure to laws and regulations in data privacy, cybersecurity, and respective industry domain

Pay close attention to developments in privacy and data protection, being a domain significantly influencing AI governance



Be guarded against algorithm disgorgement – apart from fines, regulatory actions in terms of compulsory data sets erasure may be detrimental to a company's business model itself

Be aware of multiple agencies overseeing, with likely overlaps in jurisdictions and expectations

Specific to preparing for the EU AI Act compliance, organizations are advised to follow a 5-step process.

AI systems inventory	AI Risk Classification	AI Risk Mitigation	Assessments	Governance
Create and maintain thorough inventories of AI systems	Create a risk classification system in line with the EU AI Act	Implement risk-mitigation procedures and independent audits	Conduct conformity assessments of high-risk AI systems on a regular basis based on internal and external classifications to make sure the systems adhere to regulations and, more significantly, to identify any potential negative effects	Create a cross-functional team with experts in risk management, law, and technology to establish development and deployment standards, and track compliance

Considering how GDPR as a comprehensive regulation has influenced the global privacy regulatory landscape and as fundamental aspects remaining same across jurisdictions, the above pointers could serve as a global reference as well.

Conclusion

AI (especially Generative AI) is rapidly evolving, and here to stay. It is also expected to be a significant catalyst boosting cloud adoption, helping drive another wave of digital transformation/innovation and productivity enhancement. Like any innovation in human history, it is upto the society and government to find ways and means to bring in checks and balances (some voluntary and some others enforced) to ensure the positive aspects are maximized and ill-effects are controlled. There has been gradual progress in this front over the years and with industry and governments collaborating further, we expect this accelerating further in the times to come. These interventions are expected to aid in assuring digital trust to all stakeholders, as organizations and the society at large navigate their next in their digital transformation journey which has been progressing rapidly in the recent decades.

References:

https://corporatefinanceinstitute.com/resources/economics/industrial-revolution/

https://spectrum.ieee.org/state-of-ai-2023#toggle-gdpr

https://aiindex.stanford.edu/report/

https://www.weforum.org/agenda/2022/03/designing-artificial-intelligence-for-privacy/

https://www.forbes.com/sites/larryenglish/2023/06/16/ai-and-security-is-your-organization-ready/?sh=5b0c209c530f

https://www.britannica.com/technology/artificial-intelligence/Methods-and-goals-in-AI

https://mytechdecisions.com/compliance/chatgpt-and-generative-ai-a-game-changer-but-issues-persist/

https://pages.awscloud.com/Realizing-a-cloud-enabled-economy-AWS-Accenture-2023-learn.html#:~:text=Conducted%20by%20Accenture%2C%20the%20%E2%80%9CRealizing%20a%20cloud-enabled%20economy%3A,employment%20on%20average%20across%20the%2012%20countries%20studied

https://www.forbes.com/sites/forbestechcouncil/2023/04/19/exploring-the-security-risks-of-generative-ai/?sh=7a7be4413594

https://www.gartner.com/en/newsroom/press-releases/2023-04-20-why-trust-and-security-are-essential-for-the-future-of-generative-ai

https://www.gartner.com/en/articles/what-it-takes-to-make-ai-safe-and-effective

https://iapp.org/news/a/generative-ai-privacy-and-tech-perspectives/

https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

https://www.smartnation.gov.sg/initiatives/artificial-intelligence/

https://www.nist.gov/itl/ai-risk-management-framework

https://www.goodwinlaw.com/en/insights/publications/2023/04/04_12-us-artificial-intelligence-regulations

https://iapp.org/resources/article/us-federal-ai-governance/

https://iapp.org/news/a/ai-regulatory-enforcement-around-the-world/

About the Authors

Oommen Thomas

Group Project Manager & Head of Cybersecurity GRC Practice

Oommen Thomas manages key strategic initiatives for the Cyber Security Practice at Infosys, including leading the GRC practice across GTM and Delivery CoE – devising and executing strategies for industry leading offerings and optimal business aligned solutions for global customers. He is an enthusiast on innovations in the Cyber Security, Governance Risk and Compliance, and Data Privacy domains, and has been actively associated with security/privacy/management communities including through forums like ISACA, IAPP and PMI. A continuous learner with over 3 decades of IT industry experience spanning multiple domains, geographies, roles, and functions, Oommen's industry certifications include CISSP, CGEIT, CRISC, CISM, CSX-P, CPISI, ISO27001-LA, DP/GDPR-LI, CIPP/E, CIPM, FIP, TOGAF, PMP and ITIL. He volunteers for IAPP serving on their Diversity in Privacy Advisory Board, and earlier served as Co-Chair for the IAPP Pune Chapter.

For more information, contact askus@infosys.com

Infosys®
Navigate your next