May 2023

# THE TECHNOLOGY NEWSLETTER

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA

## INTRODUCTION

The Argus Technology Newsletter discusses recent developments in technological advances or milestones or events. As lawyers, we enjoy delving into the legal nuances and implications of technological changes and analysing their impact on our clients and their activities. It is said that law always lags behind technological advances and there could be some truth behind such statement, but there is no reason for lawyers to lag behind technological advances.

The Argus Technology Newsletter is not meant to be a substitute for your regular technology periodical. Instead, we hope and promise to offer a lawyer's insights into technological change and innovation.

Argus Partners has a developed a strong and a robust technology and data privacy practice, which spans transactional advisory, corporate and regulatory advisory as well as contentious matters and disputes. Whilst physically the attorneys are based out of our Mumbai, Delhi & Bangalore offices, the team is servicing clients across the globe on Indian legal issues in technology and data privacy.

# Expectations From The Proposed Digital India Act

***Contributed by Anushkaa Shekhar (Associate)***


Currently, the Information Technology Act, 2000, which came into effect on October 17, 2000 ("**IT Act"**) is the primary legislation governing and regulating digital activities in India. Despite undergoing several amendments in the last two decades, the IT Act has become obsolete since the fundamental principles of the IT Act were established prior to the emergence of e-commerce and social media platforms. Although these digital services have enabled citizens to access healthcare, education, and entertainment through online channels, they have also presented challenges such as cybersecurity threats, data privacy concerns, and the proliferation of hate speech and fake news. The IT Act has not been able to tackle issues arising out of recent innovations such as e-commerce, social media platforms, online gaming portals, AI tools and the metaverse. As such, a new digital law that aligns with global standards and modern technologies, is long overdue.

The Ministry of Electronics and Information Technology ("**MeitY**") has been talking about a the Digital India Act ("**DIA**") that will replace the IT Act and in March, 2023 MeitY released a presentation ("**Presentation**") to inform stakeholders about the proposed new legal framework for India's burgeoning digital technology ecosystem, which will be encompassed in the Digital India Act ("**DIA**"). According to the Presentation, the DIA is expected to establish a regulatory framework for digital technologies and services in India, covering a wide range of areas, including data protection, cybersecurity, e-commerce, digital payments, and artificial intelligence, among others. Although a draft of the DIA has not yet been made public, the Presentation by MeitY provides an insight into the framework of the proposed DIA which would evolve through rules, and address the following tenets of Digital India:

- Open Internet
- Online Safety and Trust
- Accountability and Quality of Service
- Adjudicatory mechanism
- New Technologies

The main objectives of DIA include:

- Protecting user privacy and data: The proposed DIA is expected to establish clear guidelines for data protection and privacy and create mechanisms for the secure handling of user data. This would help prevent the misuse of personal information and improve trust in digital services. The DIA also aims to regulate wearable tech such as spy camera glasses by mandating strict KYC requirements for retail sales and appropriate criminal law sanctions.

- Strengthening cybersecurity: The proposed DIA aims to enhance cybersecurity measures to protect against cyber threats and attacks. This includes measures to prevent data breaches, cybercrime, and other online threats.

- Promoting digital innovation: The proposed DIA is expected to provide a conducive environment for digital innovation, by establishing clear rules and guidelines for the development of new technologies and services such as autonomous systems/robotics, virtual reality/augmented reality, real-time language translators.

- Boosting e-commerce: It is now beyond question that influential internet giants like Twitter, Facebook, and Google have a significant impact on a nation's social, economic, and political consequences. In India, the lack of regulation of social media has enabled freedom of expression but also created problems such as online harassment and hate speech. The proposed DIA aims to prevent these distortions through the regulation of dominant ad-tech platforms etc. and promoting start-up India via non-discriminatory access to digital services and interoperable platforms. This will consequently promote the growth of e-commerce in India by creating a level playing field for all market players and ensuring fair competition.

- Enhancing digital literacy: The proposed DIA is expected to include measures to promote digital literacy and awareness among the general public, to ensure that everyone can benefit from digital technologies.

- Protecting minors: The proposed DIA seeks to protect minors' data, safety, and privacy on social media platforms, gaming, and betting apps through age-gating and regulation of addictive technology. It also includes a mandatory “do not track” requirement to prevent children from being targeted for advertising purposes.

Overall, the proposed DIA is expected to play a crucial role in transforming India into a digital economy and promoting the growth of digital technologies and services in the country.

Although the proposed framework for the DIA appears promising, it is important to note that it is still in the early stages of development and details of the proposed legislation provided in the Presentation are subject to change. To ensure public safety in an increasingly digitized world, it is crucial for the proposed DIA to be promptly enacted as a legislation and implemented at the earliest.

# Google v. Competition Commission Of India – A Case Review

***Contributed by Aarti Sonawane (Associate)***


The Competition Commission of India ("**CCI**") had on October 20, 2022, passed an order against Google LLC and Google India Private Limited ("**Google**") directing Google to refrain from indulging in anti-competitive practices that were found to be in contravention of the provisions of the Competition Act, 2002 ("**Competition Act**") and also imposed on Google a penalty to the tune of INR 1337.76 Crores.

Google filed an appeal with the National Company Law Appellate Tribunal ("**NCLAT**") against CCI's order.

Google contended that CCI's order suffered from confirmation bias and that agreements executed with equipment manufacturers did not prevent them from pre-installing competing apps with similar functionality. Google further argued that its popularity was due to its effectiveness and that dominance in the market did not necessarily constitute abuse of dominance.

CCI, on the other hand, contended that Google controlled nearly 98% of the market in India for smartphone apps and was found to be violating competition laws to maintain its dominance in the market. CCI accused Google of unfair trade practices by restricting the entry of other applications in the Google Play Store. CCI summed up Google's policies in India in 5 phrases, namely "digital feudalism," "digital slavery," "technological captivity," "chokepoint capitalism," and "consumer exploitation."

CCI observed that by using its dominant position in the online search market, Google was denying access to competing search engines. It also noted that by making pre-installations of Google's proprietary apps mandatory in an android phone, the incentive and ability of device manufacturers to develop and sell devices operating on alternate versions of android was considerably reduced. Therefore, CCI directed Google to not force Original Equipment Manufacturers ("**OEMs**") to pre-install a bouquet of applications, not offer any monetary or other incentives to OEMs for ensuring exclusivity for its search services, and not restrict the uninstallation of its pre-installed apps by the users.

After hearing arguments from both sides, the NCLAT, on March 29, 2023, upheld[1] CCI's decision and ruled that Google had perpetuated its dominant position in the online search market, resulting in the denial of market access to other competing search apps. The NCLAT, however, deleted certain directions of the CCI in paragraph nos. 617.3, 617.9, 617.10, and 617.7 of CCI's order. NCLAT upheld other directions given by CCI, including the imposition of a fine on Google to the tune of INR 1337.76 Crores.

This NCLAT ruling highlights the ongoing debate surrounding anti-competitive practices and market dominance in the technology industry. Google's dominance in the smartphone apps market in India and its control over the online search market were key factors in this case. The ruling serves as a reminder to tech giants that market dominance comes with a responsibility to operate fairly and to avoid engaging in anti-competitive practices that restrict competition and harm consumers. As the technology industry continues to evolve, it will be essential for companies to operate in a manner that fosters fair competition, innovation, and consumer protection.

[1] *Google LLC and Another* v. *Competition Commission of India Through its Secretary and Others*, 2023 SCC OnLine NCLAT 147.

# International Developments in Data Privacy Laws – A Roundup

***Contributed by Paridhi Jain (Associate)***


**Developments in Vietnam:**

On April 17, 2023, the Government of Vietnam issued a long-awaited regulation on data privacy, through Government Decree No. 13/2023/ND-CP ("**Decree 13**"). Until now, Vietnam did not have a comprehensive legislation regulating the collection and processing of personal data. Instead, rules and regulations on personal data protection were present in general laws such as the Civil Code 2015 and the Law on Cyber Information Security No. 86/2015/QH13.

Decree 13, much like the European Union's General Data Protection Regulation ("GDPR"), incorporates the concepts of data processor, data controller and data subject. It classifies personal data as "basic personal data" and "sensitive personal data" and outlines personal data processing principles, including lawfulness, transparency, purpose limitation, confidentiality, accountability, and storage limitation. Similar to the GDPR, Decree 13 stipulates data subjects' rights, including the right to be informed, the right to consent, access, opt-out, erasure, restriction of processing, data portability, and the right to claim damages. Decree 13 also imposes restrictions on cross border data transfers and provides that a transfer impact assessment must be done for outbound transfers of personal data from Vietnam. There are also special provisions relating to data processing for marketing and advertising which require data subject's consent.

Decree 13 is expected to clear the ambiguity around data privacy regulation and advance Vietnamese individuals' right to privacy. It will also have considerable and wide-reaching implications on companies collecting and processing the personal data of Vietnamese citizens.

**Developments in Nepal:**

The Nepal Telecommunications Authority ("NTA") on April 22, 2023, released a regulatory framework for Internet of Things ("**IoT**") and Machine to machine ("**M2M**") service providers ("**Framework**"). The regulatory Framework unveiled by NTA covers the issuance of licenses to IoT and M2M service providers. Recognizing the significance of data privacy and security, the Framework directs IoT/M2M service providers to follow industry best practices and the applicable laws of Nepal for data security. While dealing with personal data, the Framework mandates personally identifiable information of the IoT/M2M users to be properly encrypted and to not be accessible to third parties under any circumstance. The Framework further restricts the transfer of data and specifically requires that personally identifiable information of IoT/M2M Users should be stored within Nepal. With respect to data storage and maintenance, the Framework directs IoT/M2M service providers to follow existing data telecommunication rules. Incidents of data breach are required to be reported to the relevant authority immediately and prompt technological and/or legal actions are required to be taken.

In 2015, Indian government had released a draft 'Internet of Things Policy' to promote the creation of an IoT ecosystem and development of IoT products specific to Indian needs. In February 2022, the Department of Telecommunications (DoT) issued guidelines for registration of M2M service providers. However, to date India does not have a comprehensive law regulating the IoT and M2M technologies. The rising use of IoT devices raises serious privacy concerns as IoT devices such as e-health devices, smart watches and trackers contain sensors which collect and transfer data about an individual's daily habits, activities and preferences. It is essential to regulate the manner in which such devices use and maintain data security. It is high time the Indian policy and regulatory framework catches up with these emerging technologies.

# Twitter Threatened With €50 Million Fine In Germany For Failing To Tackle Illegal Content

***Contributed by Tweesha Gosar (Associate)***

On April 4, 2023, Germany's Federal Office of Justice ("**BfJ**") initiated proceedings against Twitter International Unlimited Company ("**Twitter**") on allegations of "systemic failure" to deal with illegal content as prescribed under Germany's Network Enforcement Act ("**NetzDG**").

Unlawful content is defined by Section 1(3) of the NetzDG as content that breaches specific provisions of the Criminal Code (StGB), such as the rules on slander in Article 185 of the StGB and certain criminal law provisions on protection from threats to the democratic rule of law.

Section 3(2) of the NetzDG provides that in case of any compliant, the provider of a social network shall either:

(i) in case the content is 'manifestly unlawful', remove/ block access to the content within 24 (twenty four) hours of the social network provider receiving such compliant; or

(ii) remove/ block access to unlawful content immediately, i.e. generally within 7 (seven) days of receiving the complaint.

Section 1(1) of NetzDG provides that the aforementioned provisions shall be applicable to telemedia service providers that operate social networks for profit-making purposes, like Twitter.

Recently various complaints were filed with Twitter in Germany regarding content published on Twitter, which the BfJ feels was either unlawful or even manifestly unlawful. However, no action was taken by the tech giant in relation to the same, as required under Section 3(2) of the NetzDG.

Section 4 of the NetzDG provides that a failure to company with section 3 of the NetzDG would constitute a regulatory offence and a fine of up to fifty million euros may be imposed. Although no such fine has been levied yet, if the BfJ comes "*to the conclusion that the accusation of*

*illegal behavior is still justified, the BfJ will apply to the Bonn district court to initiate preliminary ruling proceedings and at the same time present the provider's statement*."

Although the reason for non-removal of the content is still unknown, it may be borne in mind that discussions on the commercial and ethical implications of mass firing of employees of Twitter were making the rounds around the same time. The regulatory requirements of every country differs from other countries. With tech companies growing at an exponential rate, they focus on standardizing processes and decisions globally, which may affect their ability to factor in variations in regulatory approaches between different countries.

# Global Trends In The Regulation Of AI

***Contributed by Vasavi Khatri (Associate)***

Artificial Intelligence (AI) is rapidly changing our world, from improving healthcare to enhancing transportation systems. However, with the increasing impact of AI, the regulation of its development and use has become a major concern for governments and international organizations. The regulation of AI is essential to ensure that the technology is developed and used in a responsible and ethical manner. In recent years, global trends in the regulation of AI have been emerging, with different countries and regions taking different approaches to address the challenges posed by this technology.

The Indian government sees AI as a "kinetic enabler" and seeks to harness its potential for better governance. As per Ministry of Electronics and Information Technology ("**MeitY**"), AI can be used to provide personalized and interactive citizen-centric services through Digital Public Platforms. [2] The Indian government is not considering bringing a law governing AI as of now.[3] This, however, does not mean no regulation at all. Regulation of AI presently is undertaken via regulations on issues like intellectual property, privacy and cyber security. The Indian government has also undertaken several other initiatives to enable the AI ecosystem in the country to thrive. In 2018, NITI Aayog published its discussion paper titled National Strategy for Artificial Intelligence identifying healthcare, education, agriculture, smart cities and mobility as some of the sectors for deployment of AI. MeitY has also operationalized a clutch of Centers of Excellences (COEs) to assist in knowledge management and creating capabilities to capture new and emerging areas of technology.

There have been attempts made by other regulators to initiate a discussion on the utilization of these technologies. For instance, Securities and Exchange Board of India (SEBI) has proposed to use AI for data analytics and pattern recognition to aid the regulator in identifying fraudulent behaviour and abnormal trading. The Reserve Bank of India (RBI) has also given

---

[2] "*Generative Artificial Intelligence*", Press Information Bureau, Ministry of Electronics and Information Technology, (February 3, 2023) available at https://pib.gov.in/PressReleasePage.aspx?PRID=1896016.

[3] "*Government Not Considering Regulating AI Growth, Says IT Minister Vaishnaw*", Economic Times (April 5, 2023) available at https://economictimes.indiatimes.com/news/india/government-not-considering-regulating-ai-growth-says-it-minister-vaishnaw/articleshow/99273629.cms?from=mdr.

an expression of interest for engaging consultants in the use of AI and machine learning, and advanced analytics.

In recent discussions on the Digital India Act ("**DIA**"), which is being created as a comprehensive legal framework for the digital ecosystem, MeitY stated that the proposed law would regulate "high risk AI systems" through legal, quality testing framework to examine regulatory models, algorithmic accountability, zero-day threat & vulnerability assessment, examining AI based ad-targeting, content moderation, etc. However, this proposed law does not specifically address the challenges created by use of AI.

The European Union proposes to create a comprehensive and substantial legal framework to govern AI. The EU's proposed Artificial Intelligence Act ("**AIA**") contemplates a graded regulation, i.e., regulation of AI based on its potential risks. The AI systems that are perceived as a threat to safety, livelihood of people and human rights are prohibited under this framework. They are placed in the "unacceptable risk" tier. This includes AI processes that have the potential to manipulate people, or that which may exploit vulnerabilities of specific groups, such as persons with disabilities. The AI systems which are not prohibited are categorized into "high-risk", "limited risk" and "minimal risk". The AIA is subject to EU's legislative process and may be amended in the coming years.

Australia is another jurisdiction that is grappling with regulatory issues surrounding AI. While there is no legislation which specifically deals with AI in Australia, the Privacy Act Review Report 2022 ("**Review Report**"), if adopted, may have some implications on the use of AI. The Review Report recommends that entities be required to disclose how personal information would be used in automated decisions. The black box effect in AI systems makes it difficult to regulate automated decisions because the decision-making process is not transparent, and the rationale behind the decisions is not always clear. This lack of transparency and interpretability can create ethical, legal, and regulatory challenges, particularly when it comes to ensuring fairness and preventing discrimination in decision-making.

AI and machine learning are increasingly being used for individual profiling, based on data such as behavioral trends, location, education, and purchasing history. This profiling can be used to make decisions about product and service offerings, but can also lead to bias in areas such as recruitment, and can be used for surveillance purposes. Additionally, non-consented use of AI for aggregating data and extracting health information can unfairly influence opinions, choices, and offers made to individuals by businesses, and the opaque nature of AI algorithms can make it difficult to determine how data is being used. These issues highlight the need for regulation and ethical considerations in the use of AI for individual profiling and other purposes.

Governments and legal systems worldwide are struggling to deal with the challenges posed by the black box effect and the use of AI in decision-making, particularly when it comes to protecting privacy rights and ensuring fairness and accountability.

Amidst these debates on regulation of AI, Elon Musk and others have been voicing concerns over the rapid development of AI, highlighting the dangers it poses to human civilization. There is a growing fear that AI may eventually outnumber and outsmart human minds. An open letter endorsed by the likes of Elon Musk, Steve Wozniak and Yuval Harari has suggested a pause on training systems more powerful than GPT-4 so that AI is made more transparent, safe and loyal.

# UK Digital Markets, Competition and Consumers Bill

***Contributed by Dileep Krishnan (Associate)***

On April 25, 2023, the Government of United Kingdom ("**UK**") published the Digital Markets, Competition and Consumers Bill ("**Bill**"). The Bill is undoubtedly the most important legal reform made to the competition and the consumer law regime in the UK since the setting up of the Competition and Markets Authority ("**CMA**") in 2014. The Bill aims to boost competition in digital markets which are currently dominated by a few global giants and also aims to help consumers by cracking down on unfair business practices.

The Bill significantly strengthens the powers of the CMA in relation to the regulation of competition in digital markets and enforcement of consumer law. The new rules permit the CMA to decide when a consumer law is breached without taking the matter to the court. The Bill also permits the CMA to impose monetary sanctions on businesses which are found to be in breach of the law.

Some of the key takeaways from the Bill are as follows:

1. The Bill empowers the Digital Markets Unit ("**DMU**") within the CMA to designate certain companies with "*strategic market status*" ("**SMS**") in relation to particular digital activities. A discretionary power is vested with the DMA to determine whether a particular company has SMS in relation to a given digital activity. This classification is made on the basis of factors like (i) whether the company has "*substantial and entrenched*" market power, which is to be determined basis a forward-looking assessment carried out by the CMA for a period of at least 5 (five) years, (ii) the company's "*strategic significance*" in relation to the digital activity, (iii) the company's global and UK turnover (where the threshold is met if the global turnover of the group in the relevant period exceeds 25 (twenty five) billion pounds or if the UK turnover of the group in the relevant period exceeds 1 (one) billion pounds), and (iv) whether the activity has a UK nexus.

2. A company identified as having an SMS ("**SMS Company**") will be subjected to an enforceable code of conduct tailor-made for that particular company which is designed to address the harms associated with the activities of that particular SMS Company.

The Bill sets out an exhaustive list of conduct requirements that the CMA can impose on an SMS Company, which includes requiring the SMS Company to trade on fair and reasonable terms, to present to the users/ potential users with options or default settings in relation to a relevant digital activity in such a way that it allows the users to make informed and effective decisions in their own best interests, to ensure fair usage of the data available to the company, or to enable the users to use products of other undertakings.

3. The Bill also empowers the CMA to make targeted "*pro-competition intervention*" ("**PCI**") in the functioning of an undertaking if the CMA has reasonable grounds to consider that a factor or combination of factors relating to a relevant digital activity may be having an adverse effect on competition. PCI aims to address the market dominance of the SMS Companies. The scope of PCI is so wide that the CMA can make a PCI for the purposes of remedying, mitigating or preventing any detrimental effect on UK users that the CMA considers has resulted, or may be expected to result, from the adverse effect on competition.

4. In addition to this, the Bill also prescribes stricter compliance norms for the SMS Companies which includes a mandatory requirement to report certain transactions to the CMA prior to completion. The aim is to monitor any possible mergers which may have an adverse effect on the UK consumers and businesses. Once the transaction is reported, the same will be assessed by the CMA before accepting the report and a transaction cannot be completed until the CMA has accepted the report.

5. Another significant feature of the Bill is the strengthening of the enforcement powers of the CMA. The Bill empowers the CMA to impose orders to comply, provide for monetary sanctions for breach of law (up to a tune of 10% (ten per cent) of the company's annual turnover globally) and for failure to comply with investigations, to disqualify the directors for instances of serious breaches etc. The enforcement decisions of the CMA will be subject to an appeal only based on the judicial review principles. This limits the judicial intervention and will provide greater autonomy, independence and discretion to the CMA in its decision making.

6. The Bill also seeks to protect consumers' collective interests. The Bill empowers the CMA to enforce the consumer laws directly through the administrative proceedings without the intervention of courts. Further, the CMA will be able to intervene in cases of new age consumer harms such as fake reviews, subscription contracts etc.

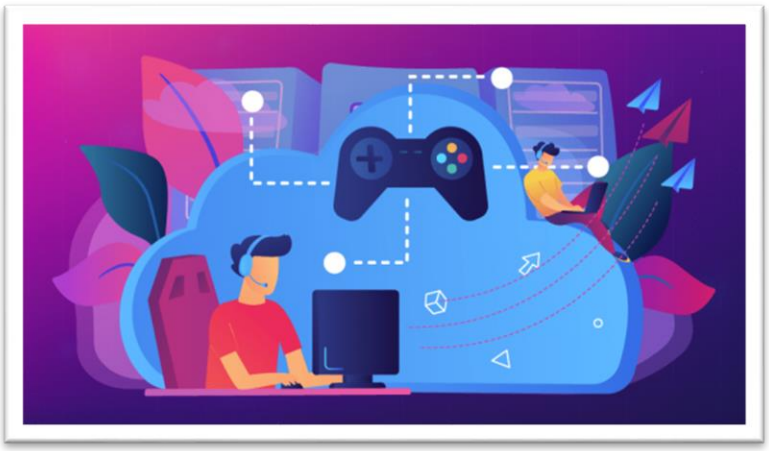
## Conclusion

The reforms proposed to the UK's competition and consumer law regime will have a profound impact across all the businesses carried out in UK. To a large extent, these proposals follow a legislative intent similar to that of the EU Digital Markets Act ("**EU DMA**") which will come into force within the European Union from May 2, 2023. However, the Bill provides much greater flexibility in its approach than the EU DMA. The EU DMA follows a legislation driven approach wherein the legislation identifies certain enterprises as "*gatekeepers*" basis their size and once this classification is made, those enterprises shall comply with the legislated code of conduct. On the other hand, the Bill provides greater regulatory discretion wherein the regulator (CMA) determines if an enterprise has SMS and if so, will provide tailor specific remedies to that particular SMS Company. The risk of such distinction in the approaches of different regulators is that it may create parallel and overlapping obligations which can lead to conflicting outcomes which may in turn result in a disruptive environment for both the

enterprises and the consumers. Nevertheless, it is an undeniable fact that the EU DMA and the proposed Bill will have a first mover advantage in the regulatory marketspace and the policies adopted by these legislations will pave way for setting up the international standards for other countries to follow.

# Regulation of online gaming through the Intermediary Guidelines

***Contributed by Smriti Tripathi (Senior Associate)***



On April 6, 2023, the Ministry of Electronics and Information Technology ("**Ministry**") notified the amendments ("**Amendment**") to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**Intermediary Guidelines**") to regulate online gaming. This article seeks to analyse the Amendment on the following two issues:

a) Overlap with the powers of the state legislature to regulate betting/gambling; and
b) Distinction between a game of skill and a game of chance.

**Overlap with the powers of the state legislature to regulate betting/gambling**

The Indian Constitution envisages a federal system wherein legislative powers have been divided between the Centre and the States. Such division of powers has been laid down in Article 246 read with the Seventh Schedule of the Indian Constitution. The Seventh Schedule contains three lists: (i) the Union (Central) List comprising subjects on which the Centre alone is empowered to legislate, (ii) the State List, comprising subjects on which the States alone may legislate (barring a few exceptions) and (iii) the Concurrent List, which contains subjects on which both the Centre as well as the State governments may legislate.

Entry 34 in the State List provides for betting and gambling. Accordingly, most States have promulgated their own statutes for regulation of betting and gambling. A majority of these State laws have banned 'gaming', which is defined as any type of wagering or betting other than wagering or betting on a horse race and excluding lotteries. For example, in terms of Section 2(7) of the of the Karnataka Police Act, 1963 ("**KPA**"), which regulates gaming in Karnataka, a lottery is expressly excluded from the definition of "gaming" but all forms of wagering or betting in connection with any game of chance (except such wagering or betting on a horse-race run on any race-course within or outside the State, which satisfies certain specified conditions) are included within the definition of "gaming". Under the KPA, any person who keeps or uses a place for the purpose of a common gaming house or any person who is found in any common-gaming house gaming shall, on conviction, be punished with imprisonment.

Further, under most state laws, games of skill have specifically been excluded from the definition of 'gaming'. However, in some States, like Sikkim, gambling is legal.

Furthermore, since most of the state laws on gaming are pre-internet, they do not envisage online gaming. Sikkim is again an exception here, since Sikkim has laws to regulate online gaming: The Sikkim Online Gaming (Regulation) Act, 2008 ("**SOGA**") read with the Sikkim On-Line Gaming (Regulation) Rules, 2009 ("**SOGR**"). In terms of Section 2(d) of SOGA, "online games" means all or any games of chance or a combination of skill and chance, including but not limited to poker, roulette, blackjack or any game, played with cards, dice or by means of any machine or instrument for money or money's worth, as may be prescribed from time to time. Section 3(2) of SOGA states that no online games shall be played, organized or exhibited to any person at any public place, except through online gaming website in respect of which license is granted in accordance with the provisions of SOGA and such license is in force.

The notification of the Amendment has raised an important constitutional question – whether the central government by notifying a framework for online gaming, has encroached upon the powers of the state governments?

An argument may be made that the Amendment has been notified by relying upon the Centre's residuary powers of legislation, which has been provided in Article 248 read with Entry 97 in Union List of the Seventh Schedule of the Indian Constitution. Article 248 (1) states as follows: "*Subject to article 246A, Parliament has exclusive power to make any law with respect to any matter not enumerated in the Concurrent List or State List*." Entry 97 in the Union List specifies "*any other matter not enumerated in List II or List III including any tax not mentioned in either of those Lists*."

Therefore, the central government may legislate on any matters which have not been specifically included in any of the lists in the Seventh Schedule. While this may, *prima facie*, provide a reasonable explanation for the central government's approach, there is an inherent flaw in this argument. As per this logic, the central government would be empowered to legislate on all the matters which came up after adoption of our Constitution or matters that could not even have been envisioned at the time of drafting the Constitution. This would include information technology, e-commerce, cyber laws, data protection, robotics, artificial intelligence, cryptocurrency, social media, sustainability, climate change etc. One look at this list and one can ascertain that a lot of the most pressing issues in today's age would fall under the centre's "residuary powers", if we adopt a literal interpretation of Article 248 and Entry 97 in Union List of the Seventh Schedule of the Indian Constitution. This could not have been the legislative intent of the founding fathers of the Indian Constitution.

A counter argument may be made that merely because an item does not feature in any of the three lists, it does not mean that such item automatically falls within the residuary powers of the Centre. Rather, one must look at the core/essence of the matter to determine in which list such matter truly belongs. Support may be taken from the doctrine of "*pith and substance*", which has been adopted and evolved by the Indian courts to resolve Centre-State conflicts regarding their respective legislative competence. Under this doctrine, when a legislature's legislative competence to enact a particular law is challenged with reference to entries in different legislative lists, the courts endeavour to determine the essence and true nature of the legislation, irrespective of its nomenclature. If the essence of the challenged law falls within the competence of the legislature which has enacted that law, then the validity of such law is upheld even if it slightly encroaches upon or touches a subject matter which is not within the legislative competence of such legislature. It is interesting to note that not only "betting and gambling" (entry 34) but also "sports, entertainments and amusements" (entry 33) feature in the State List. If we analyse the Amendment, it is apparent that one of its primary objectives is to ban any online real money game that involves wagering. Another objective is to regulate online games (which are nothing but games offered on the internet) and entities offering such online games. While the first objective falls squarely within the State List, even games which are a form of entertainment/amusement, should logically fall within the State List.

A related question worth exploring is whether the operator of an online game that complies with the Intermediary Guidelines can operate across India, irrespective of state laws? Can a "permissible online real money game" verified by an OGSRB operate in Karnataka even if such permissible online real money game violates the KPA?

Article 254 of the Constitution purports to deals with such a situation. Article 254(1) states as follows: "*If any provision of a law made by the Legislature of a State is repugnant to any provision of a law made by Parliament which Parliament is competent to enact, or to any provision of an existing law with respect to one of the matters enumerated in the Concurrent List, then, subject to the provisions of clause (2), the law made by Parliament, whether passed before or after the law made by the Legislature of such State, or, as the case may be, the existing law, shall prevail and the law made by the Legislature of the State shall, to the extent of the repugnancy, be void*."

Does it mean that all provisions of the existing state laws that are contrary to the Amendment shall be void, to the extent of contradiction/repugnancy. However, such a result follows only when a state law contradicts a law made by the Parliament *"which Parliament is competent to enact".* Which brings us back to the question on whether the Parliament has acted within its legislative competence.A middle approach may be to take a view that while States are still free to regulate offline gaming and gambling as per their legislative wisdom, online gaming should be regulated by central laws, since these games are offered over the internet and it may not be administratively feasible to enforce different state laws for such games. However, this may result in an absurdity: while offline gambling may be legal in a State, online gambling will not be legal in such a State. This differentiation based only upon the mode of offering the games, may not stand scrutiny in a court of law.

More clarity is need on the afore-mentioned issues.

**Distinction between a game of skill and a game of chance**

Rule 4A(3) of the Intermediary Guidelines (as inserted by the Amendment) provides that an OGSRB may declare an online real money game as permissible online real money game, if after making necessary inquiries, it is satisfied that (i) the online real money game does not involve wagering on any outcome; and (ii) the online gaming intermediary and such online game is in compliance with the provisions of Rules 3 and 4 of the Intermediary Guidelines, the provisions of any law relating to the age at which an individual is competent to enter into a contract, and the framework made by the SRB under Rule 4A(8) (which relates to framework for verifying an online real money game).

Thus, the Amendment has banned any online real money game that involves wagering on any outcome, without giving a precise definition of 'wagering'. Further, it appears that if an online real money game involves any wagering, it shall not be eligible to be verified as a permissible game, even if the game if predominantly a game of skill.

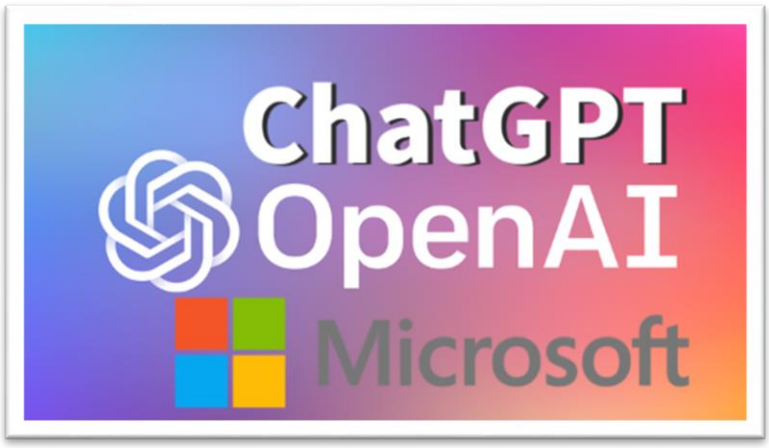
This approach would be in stark contrast to the verdict given by the Madras High Court in *Junglee Games v. State of Tamil Nadu* and the Kerala High Court in *Head Digital Works Private Limited v. State of Kerala,* wherein the courts have distinguished between games of skill and games of chance and have held any prohibition on the former to be ultra vires the Constitution. A similar judgment was delivered by the Karnataka High Court in *All India Gaming Federation* v. *State of Karnataka* (Writ Petition Nos. 18703, 18729, 18732, 18733, 18738, 18803, 18942, 19241, 19271 19322, 19450 and 22371/2021 (GM-POLICE)), wherein the Karnataka HC, referring to the difference between a game of chance and a game of skill, held as follows: "*The distinction lies in the amount of skill involved in the games. There may not be a game of chance which does not involve a scintilla of skill and similarly, there is no*

*game of skill which does not involve some elements of chance. Whether a game is, a 'game of chance' or a 'game of skill', is to be adjudged by applying the Predominance Test: a game involving substantial degree of skill, is not a game of chance, but is only a game of skill and that it does not cease to be one even when played with stakes*."

There has been much litigation on this aspect in the last few years and it was hoped that any regulation on online gaming would settle this issue; however, this Amendment appears to have missed that opportunity. We have covered these judgments in detail in our earlier updates, which may be found here and here.

# Fear v. Curiosity – OpenAI's ChatGPT

***Contributed by Jaisha Sabavala (Senior Associate)***




**What is ChatGPT?**

ChatGPT is an artificial language model developed by a company known as OpenAI, based on the GPT (Generative Pre-trained Transformer) technology. It is designed to generate human-like response writing based on the patterns and information it has learned from the training data to queries or prompts. Presently, it is in a question-and-answer format which makes it even more interesting, as if the questions are being answered by a human. ChatGPT has been trained on a massive amount of text data, allowing it to understand and generate reasoned responses to a wide range of topics. Its abilities include language translation, text completion, summarization, question answering, and more. This vast accessibility of Chat GPT comes with a vast database of knowledge feed to it.

However, with the unlimited possibilities that these applications can provide, some countries have felt threatened due to the lack of not having in place proper rules and regulations to govern the advancement of artificial intelligence. Therefore, many international forums and countries have attempted to take steps to protect their data privacy laws and have in place other laws to govern this artificial intelligence-based technologies.

**What are The Global Trends and Recent Developments?**

The Italian Government issued a report on ChatGPT and banned the use of ChatGPT in the country. However, they have recently lifted this ban. The major concern faced by the Italian government is that such AI based applications do not respect the data privacy laws of the country and there is a complete lack of transparency as to how the company stores and uses the data. This issue was also addressed by the European Union which later proposed various regulations for the same.

The UK government has a comparatively liberal approach towards the use of AI applications and has not proposed any restrictions. Although the United States of America does not have any federal laws for the use of AI, the country's National Institute of Science and Technology (NIST) does promote an AI Risk Management Framework. In India, the NITI AYOG and Planning Commission have issued guidelines on the working of such AI applications, however these are not legally binding. Countries like China, Russia, and North Korea with heavy internet censorships have altogether banned the use of ChatGPT in their countries.

**Will The Consumer Forum in India Cover The Services Provided by ChatGPT in its Ambit?**

The Consumer Protection Act, 2019 ("**CPA**"), protects consumers from any deficiency in service or any malfunctioning products. The major challenge is to determine if the user of AI / ChatGPT would fall within the definition of Consumer as provided under CPA. Section 2(42) of CPA defines a consumer, who is availing goods and services for a 'consideration' which means that the users of ChatGPT would be excluded from approaching the consumer forum since such users do not pay any fee to use ChatGPT. However, the upgraded version of ChatGPT does include paying of a subscription fee. Therefore, a user of ChatGPT could be considered as a consumer as per CPA and could approach the consumer forum. However, the disclaimers / terms of use of ChatGPT would prevent or come in way of the consumer from seeking reliefs. As per section 2(17) of CPA, Open AI would be considered to be a service provider under the electronic service provider definition and according to Section 2 (37) (ii) of CPA, Open AI would also be considered as a product seller as it includes a service provider. Would false information or a wrong factual matrix generated by AI amount to misleading the consumer or amount to deficiency in service? These questions still stand as roadblocks in determining the liability and accuracy of information provided.

**Disclaimers and Terms of Use – Do They Provide Protection to ChatGPT?**

The terms and conditions of use of AI applications are intended to reduce or mitigate the liability arising out of false content or responses generated by AI. Further, it defines the permitted conduct allowed by its user. A strong terms of use agreement is a great line of defence, but such defence is not absolute.

The important question that arises is how far these terms and conditions reduce the liability of the developers of AI applications? Would the terms and conditions be a sufficient defence if a user claims that the response generated was false / factually incorrect or misleading? A complete lack of clarity on such aspects in connection with the use of AI technologies along with its expansion bearing in mind, makes the framing of rules and regulations absolutely necessary.

**Regulatory Framework – Need Of The Hour**

Presently, there is no specific law governing ChatGPT in India. Undoubtedly, ChatGPT is a gamechanger, but there are many problems associated with its expansion. One of the major concerns with artificial intelligence is the uncertainty of the manner in which the algorithm works to generate a response and the criteria on which ChatGPT basis its replies on. If the algorithm has an inbuilt bias, it will undoubtedly lead to skewed responses. Does the answer lie in making the relevant algorithm transparent and available for scrutiny by the regulators?

Problems like accuracy of such information available, biasness of such information generated, source of such information, liability in case of relying upon such inaccurate / false information and many more issues are linked to the easy and accessible use of AIs. Further there is a lack of transparency regarding the usage and storing of data which is a major concern for data protection and privacy laws.

The recent technological developments have led to a new digital era which has opened the gates for AI development all around the world. ChatGPT is only one such application that has gained popularity and in a matter of no time there will be plenty of such applications open to public at large which may even be far advanced than what ChatGPT is today. Easy and speedy availability of information can be a major threat in the event of no stringent laws being in place imposing liabilities/responsibilities upon the developers of applications providing information through artificial intelligence technologies. Thus, a proper regulatory framework

and stringent laws and policies must be enacted and is definitely the need of the hour. Even when such laws are in place, it would be an interesting journey for lawyers, judges and the policy makers as to how such laws would be interpreted to practically implement such laws.

***Contributed By***

[Ankit Guha, Partner]

[Jitendra Soni, Partner]

[Udit Mendiratta, Partner]

[Vinod Joseph, Partner]

Jaisha Sabavala, Senior Associate

Smriti Tripathi, Senior Associate

Aarti Sonawane, Associate

Anushkaa Shekhar, Associate

Dileep Krishnan, Associate

Paridhi Jain, Associate

Tweesha Gosar, Associate

Vasavi Khatri, Associate


**MUMBAI**
11, Free Press House
215, Nariman Point
Mumbai 400021
T: +91 22 6736 2222

**DELHI**
Express Building
9-10, Bahadurshah Zafar Marg
New Delhi 110002
T: +91 11 2370 1284/5/7

**DELHI**
155, ESC House, 2nd floor,
Okhla Industrial Estate, Phase 3,
New Delhi – 110020
T: +91 11 45062522

**KOLKATA**
Binoy Bhavan
3rd Floor, 27B Camac Street
Kolkata 700016
T: +91 33 40650155/56

**BENGALURU**
68 Nandidurga Road
Jayamahal Extension
Bengaluru 560046
T: +91 80 46462300

**www.argus-p.com I communications@argus-p.com**