September 2022

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 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.

Delhi High Court directs DNRs to comply with IT Rules 2021 or face action

Contributed by Akshay Bhatia (Associate)

Background

The Delhi High Court ("**High Court**") recently had the occasion to consider the issue concerning proliferation of imposter domain names resulting in monetary loss to the general public, trademark and brand owners owing to inadequate verification of registrants and privacy protect features offered by domain name registrars ("**DNRs**"). The High Court was dealing with a batch of matters filed by trademark and brand owners alleging rampant infringement of their marks by fraudulent persons registering imposter domain names. In an order passed in *Dabur India* v. *Ashok Kumar* on September 14, 2022 ("**Order**"), the High Court has directed various DNRs to appoint grievance officers ("**GOs**") in compliance with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules 2021**").

In April 2022, the High Court in *Snapdeal Private Limited* v. *GoDaddycom LLC*, had held DNRs to be 'intermediaries' under the Information Technology Act, 2000. In July 2022, in the same litigation, the High Court had held that a plaintiff ought to identify each infringing domain name against which relief is sought and that an overarching injunction order against DNRs, without identifying specific domain names, cannot be granted. We have covered these developments previously in our April 2022 and July 2022 Technology Newsletters.

Court's observations

At the hearing, the High Court took cognizance of a) the status report filed by the Delhi Police in its probe into unlawful collection of monies by imposter domain names; b) the status report filed by the Ministry of Electronics and Information Technology

("**MeitY**") pursuant to meetings with stakeholders to consider issues such as modes of registration of domain names, verification of domain names, privacy protect features, hosting of websites on the fraudulent domain names; and c) submissions by DNRs with respect to appointment of GOs and grievance redressal mechanisms in compliance with IT Rules 2021. The High Court was of the opinion that these issues emerge from the lack of an active mechanism for identification of imposters defrauding the public of large sums of monies.

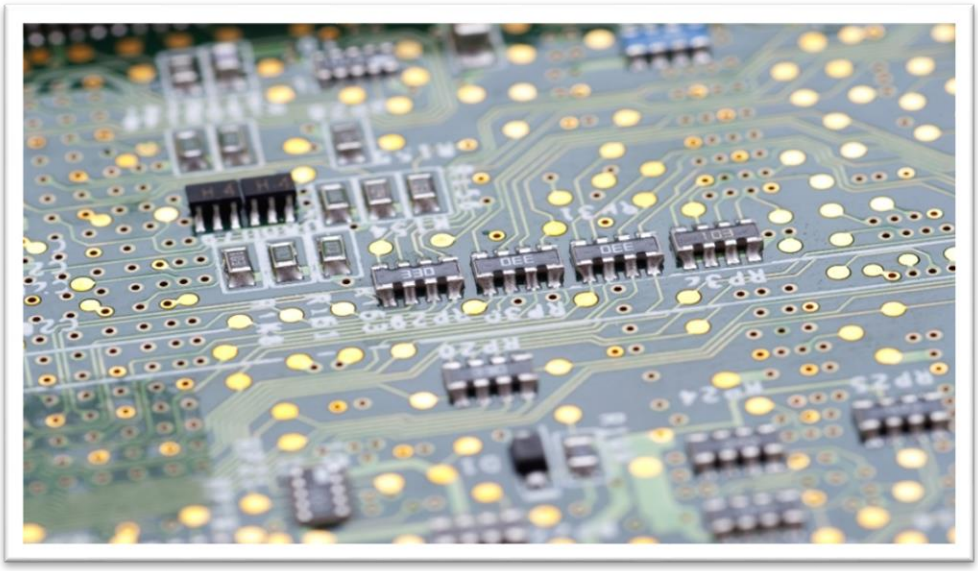
The High Court then took up the issue of appointment of GOs and grievance redressal mechanism in relation to DNRs under the IT Rules 2021. The High Court directed the MeitY to inquire into the issue of appointment of GOs of DNRs that have not responded to the High Court yet and also gave a last opportunity to DNRs such as GoDaddy, who have not appointed a GO in compliance with IT Rules 2021 despite being issued multiple directions by the High Court. Importantly, the High Court came down heavily on recalcitrant DNRs that are offering their domain name registration, hosting and related services in India without complying with local laws. The High Court stated that the MeitY and Department of Telelecommunications are free to proceed against DNRs that do not appoint GOs and are not compliant with IT Rules 2021, within one week from the date of the Order.

Conclusion

There has been a rise in the number of cases where imposter domain names lead the public to believe that websites hosted on imposter domain names belong to the actual owners, leading to monetary loss to gullible and innocent civilians as well as loss to actual trademark and brand owners. The High Court's cognizance of the lack of an effective mechanism for the identification of imposter domain names and fraudulent persons in this regard is a step in the right direction. This has also bought to the forefront, the status of compliance by DNRs with the IT Rules 2021, which has been in force for more than a year now. With the High Court directing compliance with local law obligations, specifically the IT Rules 2021, DNRs operating within India have to ensure compliance at the earliest to avoid falling foul with Indian law.

The Digital India Act: The Proposal and Prospects

Contributed by Vallari Dronamraju (Associate)



The Ministry of Electronics and Information Technology ("**MeitY**") is keen on introducing the Digital India Act ("**DIA"**) in the winter session of the Parliament in 2022. The Information Technology Act ("**IT Act**") will be replaced by the Digital India Act and address new age issues such as digital data protection and non-personalised anonymous data. As mentioned by Mr. Rajeev Chandrashekhar, the Minister of State for MeitY, the DIA will be a comprehensive legislative framework that will protect citizens' digital rights as priority. MeitY is also studying similar frameworks in place in Singapore and Australia along with Europe's GDPR. This regulation will cover the entire digital ecosystem, that will include social media platforms, OTT platforms and big tech companies.

Interplay with Competition Law

With the changing regulatory landscape in India, big tech multinationals like Google, Facebook, Twitter and Amazon have implemented policies that the competition regulatory authorities have penalized before. These have also overlapped with information technology laws. The DIA may be expected to act as a regulation that bridges this gap between competition law and information technology. The inclusion of anti-trust provisions within the ambit of the proposed DIA would increase its scope and the expansion should be undertaken after understanding the focus and assuring clarity in enforcement of such provisions. Therefore, while the bill is still awaited, we hope the DIA will be harmonious with existing and future sectoral regulations.

Data Privacy

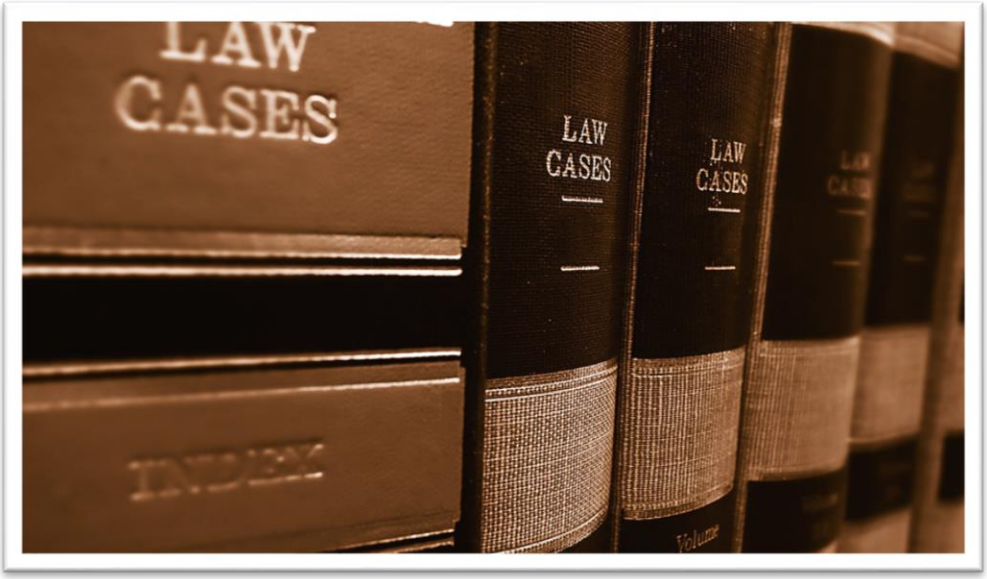
Further, the DIA proposes to have a stronger emphasis on privacy, data localization for critical data, content moderation and surveillance on cyber bullying. The government may also be looking to change the way anonymized data is looked at and democratize its usage for companies. In addition to this, the National Data Governance Framework Policy that addresses the non-personalised data and anonymous data will add to the debated Personal Data Protection Bill. The Personal Data Protection Bill was withdrawn and is to be replaced by a comprehensive legal framework on the digital ecosystem. The DIA may subsume several of these amendments. Further, under the DIA, Indian users may be given the ability to provide specific permissions to various apps they use and take away or ask the apps not to save their data or not use their personal data for any other purpose. Search engines may be asked to share data along with start-ups being given the freedom to use data for their products.

Conclusion

In today's day and age, all kinds of businesses treasure data. However, with the DIA, data sharing may become a mandate and many have also started to look for legal insulation. The DIA will also be looking into misinformation and incitement of violence as one of its primary purposes. The government will also be empowered to block Twitter handles or Facebook pages temporarily in such instances. Furthermore, the DIA is also looking to put safeguards regarding child safety and women's safety and regulation against inciting violence and spreading misinformation. The DIA is also to deal with regulating new and emerging technology in relation to blockchain and artificial intelligence. We assume that the government has factored in its previous experiences, stakeholder feedback and the proposed DIA will manage to benefit both Indian businesses as well as making the internet a safe space for Indian citizens.

Delhi High Court extends 'safe harbour' protection to intermediaries in criminal cases – a big relief for all intermediaries

Contributed by Niharika Sharma (Associate)



The Delhi High Court ("**Court**") in its recent order ("**Order**") in a petition filed by Flipkart Internet Private Limited ("**Flipkart**") has held that, 'safe harbour' protection or immunity from prosecution under Section 79 of the Information Technology Act, 2000 ("**IT Act**") is available to intermediaries even in cases of criminal prosecution.

Background

The Order has been passed in a criminal writ petition filed under Article 226 of the Constitution of India, 1950 read with Section 482 of the Code of Criminal Procedure, 1973 in the case of *Flipkart Internet Private Limited* v. *State of NCT of Delhi*. In its petition, Flipkart had sought quashing of an F.I.R registered against it by Sanash Impex Private Limited ("**Sanash**"), before the Economic Offences Wing under Section 63 of the Copyright Act, 1957 and Section 103/104 of the Trade Marks Act, 1999, alleging that Flipkart is allowing fake/ unauthorised resellers to sell fake and unauthorised products of an international Czech brand, named, 'DC Dermacol'. As per Sanash, 'DC Dermacol' had gained high repute as a global brand for skin and makeup products and that Sanash was the sole/ exclusive authorized reseller of the brand's products in India.

Before the Court, Flipkart argued that since it is an 'intermediary' under Section 2(1)(w) of the IT Act, it is entitled to safe harbour protection for any information/ data hosted by third parties on its platform in terms of Section 79 of the IT Act. Flipkart further argued that in terms of the judgment of the Supreme Court in the case of *Shreya Singhal* v. *Union of India*, until and unless a court order is served upon Flipkart,

directing it to remove from its platform certain specifically identified content, there was no obligation on Flipkart, as an intermediary, to remove any material from its portal.

Court's findings

After close scrutiny of the provisions of IT Act, Information Technology (Intermediary Guidelines) Rules, 2011 as also under the latest Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**Intermediary Guidelines**"), Copyrights Act as well as the Trade Marks Act, the Court opined that the IT Act does not provide for infringement of copyright or trademark as an offence. Compliance with the 'due diligence' requirement under Rule 3 of the Intermediary Guidelines would render the intermediary eligible for exemption from criminal liability as well. Even otherwise, non-compliance with the Intermediary Guidelines has not been declared as an offence under the IT Act.

The Court further observed that, intermediaries have been granted 'safe harbour' qua civil liability and even when a higher standard of culpability is required for criminal prosecution, such 'safe harbour' should be available even in respect of criminal prosecution. Thus, unless an active role is disclosed in the commission of the offences complained of, the intermediary would be entitled to claim protection under Section 79 of the IT Act.

On this basis, the Court quashed the F.I.R registered against Flipkart.

Conclusion

Indian law is unclear on the due diligence/ compliance requirements by e-commerce platforms to avail 'safe harbour' protection under Section 79 of the IT Act. The Order of the Court is a welcome "business friendly" decision that grants immunity to intermediary e-commerce platforms from criminal prosecution. It remains to be seen if the Order is appealed against and a different view is taken by appellate courts.

Central Bank Digital Currency – A potential privacy concern?

Contributed by Esha Dinesh (Associate)

The Supreme Court in the Pegasus Case had observed that, "*We must recognize that while technology is a useful tool for improving the lives of the people, at the same time, it can also be used to breach that sacred private space of an individual. The right to privacy is directly infringed when there is surveillance or spying done on an individual, either by the State or by any external agency*". As per Article 12 of the Universal Declaration of Human Rights Act, 1948, right to privacy is recognized as a basic human right and any arbitrary interference in one's privacy shall be considered as an attack on one's honour and reputation. The Apex Court has reiterated time and again that, the right of privacy is covered under Article 21 (*Right to life and personal liberty*) of the Constitution of India, 1950.

What is Central Bank Digital Currency?

In the spirit of giving a boost to the financial sector of India and inspired by the popularity of cryptocurrencies and digital currencies, the Finance Minister and the Reserve Bank of India ("**RBI**") are presently in the preliminary stage of introducing Central Bank Digital Currency ("**CBDC**") in India and are heading towards a nation-wide launch. CBDC is a legal tender in digital form, regulated by the central bank of the country. It shall have the same value as that of fiat currency of the country but will be in digital form stored in an electronic wallet. Across the globe, approximately 11 countries and territories have launched CBDCs and 80 countries are in the trial stage. Bahamas was the very first economy to launch nationwide CBDC – Sand Dollar. China's digital yuan CBDC was claimed to have some formidable transaction tracing capabilities and the aim of the authorities was 'controllable anonymity'. In India, 4 (four) banks, namely State Bank of India, Punjab National Bank, Union Bank of India and Bank of Baroda have been asked by the RBI to initiate the trial of CBDC.

CBDC can potentially create a greater level of resilience for payment systems and increase the efficiency and lower the costs of transactions. A nation-wide launch of CBDC shall lead us to a cashless economy and digital currencies to conduct any domestic transaction or cross border transactions which does not require any involvement of a third party or bank. Resultantly, it will also eliminate any third-party risk of events such as bank failures. As per the authorities, CBDC shall prove to be a more robust, trusted, regulated, and efficient legal tender-based payment option. RBI has been actively working towards the implementation of launch of CBDC in a phased manner.

CBDC seems promising as it would significantly save the cost of printing, storage and distribution of currency in India. However, technology has always proven to be a double-sided sword. Even though technology advancement in various sectors of economy of India has shown tremendous growth, there have been drawbacks and flaws in each such advancement, primary concern being that of data privacy and protection.

Through the operation of CBDC, the RBI will be keeping a record of every transaction taking place, increasing the surveillance across the country and implying that there will be a complete footprint of how the currency has flowed down. While this will enable the authorities to address financial crimes and act accordingly as required, it will also increase the traceability of each transaction made by each individual. This will increase the control and surveillance potential of the State and RBI significantly.

Potential risks associated with launch of CBDC

While there remains uncertainty with respect to the functioning of CBDC and the specific operating system which will be used, cyberthreats and attacks will, however, continue to grow. The State not only has to brace itself to face confidentiality issues or the development of new areas of risk for fraud or technology abuse but also, solve for accessibility with respect to majority of population of India and the possible attacks on CBDC system which will compromise not only on data security but also other aspects, including possible system failure resulting in disruptions.

Information Technology Act 2000 and Rules thereunder

The technology sector in India is governed by the Information Technology Act, 2000 ("**IT Act**") and the respective rules thereunder. The IT Act primarily governs and grants a legal recognition to all transactions and exchange of data *via* electronic platform or medium in India. While the IT Act defines the term 'data', it does not specifically provide any efficient framework for protecting such data or privacy of the respective individuals.

Considering the need to protect the data and ensure a safe system for usage, collection and storage of information of individuals, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI Rules**") was introduced. Rule 3 of the SPDI Rules which defines sensitive personal data includes financial information such as bank

account, credit card, debit card or other payment instrument details pertaining to an individual in India.

Potential role of Data Protection Bill 2019?

The Data Protection Bill 2019 ("**DP Bill**"), after being introduced, made headlines for several months, particularly for the arbitrary powers that were granted to the State with respect to processing, usage and storage of data of individuals. The DP Bill focused more on heavily regulating the provisions governing the business corporates, while granting arbitrary powers to the State which can lead to misuse of data so collected and stored. Despite the DP Bill having its own flaws which were required to be addressed, it still did not have the potential for addressing the long overhaul of safely processing of sensitive data, particularly in terms of financial information.

The DP Bill was applicable to, apart from data processed within the territory of India, any processing of personal data by the State, any Indian company, data fiduciaries (even though not present in India), or any citizen of India. On a perusal of Section 2(36), it can be understood that while personal data is the genus, sensitive personal data is the species of it. Further, the legislature, while defining the term 'data fiduciary', ensured to include State within its ambit. Furthermore, the DP Bill defined 'financial data', which is a sensitive personal data, as any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a financial institution and a data principal including financial status and credit history.

Considering the aforementioned, while the term 'financial data' would include the transactions of an individual within its scope, Section 12 under Chapter III (Grounds for processing personal data without consent) allows the State to process any personal data for execution of any function of the State which may render any service or benefit to the individual or if such processing of personal data is required under any law as may be introduced by the legislature, without any consent of the individual. Neither the provision excludes sensitive personal data from its ambit, nor does it explicitly and specifically provide for the types of services, benefits or laws and the purposes building its basis. The fact that State has the power to process such data without the consent of the individuals would have led to privacy breach of the respective individuals, more importantly because CBDC is proposed to be governed and regulated by the Central Government and RBI. Irrespective of this, the DP Bill stands withdrawn as of now.

Principles of GDPR

General Data Protection Regulation ("**GDPR**"), a regulatory framework introduced in May 2018 under European Union law, has been the most defining step in privacy and data protection. Under Article 3, the GDPR enlists its 6 principles based on which it has framed a progressive and extensive legal regime – (a) lawfulness, fairness, and transparency; (b) limitations on the purpose of collection, processing, and storage; (c) data minimization; (d) data accuracy; (e) data storage limits; and (f) integrity and confidentiality. What should be taken into note is that the GDPR takes note to limit the purpose of collection, processing and storage of such data so received. Keeping this in view, such limitation should be ideally imposed in the case of CBDC as well, which

shall limit the purpose and collection of data to the extent of as necessarily required and ensuring anonymity otherwise.

New technology law for data privacy and protection – Need of the hour

The level of technology advancement in India is increasing in all sectors. In its attempts to dump heavy compliances onto corporate bodies, the legislature conveniently missed ensuring that the individuals and their privacy with respect to data needs protection from the State as well. Considering the nature of CBDC, usage and storage of financial information of individuals and the tweaks in every technical operating system which hackers take due advantage of, launching CBDC before setting up an air-tight regulatory framework to govern the crimes associated with technology may prove to be its downfall, resulting in concerns, interruptions and a possible system crash. India is still in a need for a robust and efficient regulatory framework which will not only protect data but also provide and maintain privacy of individuals, even from the State.

To eliminate the possibility of digital frauds and cyber threat, it is crucial to take pre-emptive steps and enforce credible data protection security law. Further, it is also pertinent to analyse the extent of data that will be collected in the functioning of CBDC – whether it is limited to that of transaction details or will widen its scope to include location, personal details of individuals, bank account details in real time, etc. The threat and possibility of violation of an individual's privacy and data security is directly proportionate to the extent or the level of access that will be granted to the State in the operation of CBDC in India.

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
knowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com

Contributing Partners

Ankit Guha, Partner
ankit.guha@argus-p.com

Jitendra Soni, Partner
jitendra.soni@argus-p.com

Udit Mendiratta, Partner
udit.mendiratta@argus-p.com

Vinod Joseph, Partner
vinod.joseph@argus-p.com

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

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

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

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