Lex Spectrum
Delivering Quality

Navigating the Digital Legal Landscape - 2023

Lexspectrum, Solicitors & Advocates
A -384, First Floor,Defence Colony,Delhi -110024
Phone: 9958201822
Email: manish.gaurav@lexspectrum.in

Introduction:

The year 2023 has brought forth pivotal legal updates in the realm of information technology, reflecting the rapid evolution of the digital landscape. Governments worldwide are grappling with the challenges posed by advancing technologies, seeking to strike a balance between fostering innovation and safeguarding individual rights. This article delves into the key legal developments that have unfolded in 2023, shedding light on the intricate interplay between technology and the law.

Legislative Updates:

Following a delay spanning five years, India has enacted its own Data Protection Law, officially known as the Digital Personal Data Protection Act, 2023 ("Data Protection Act")[1].

The Government of India notified this legislation in August 2023. The Data Protection Act is applicable to the processing of personal data, whether in digital or non-digital form, and whether initially in digital form or later digitized. It extends its jurisdiction to data processing activities conducted within or outside the territory of India, provided they are related to goods and services within the Indian territory.

As defined in the Data Protection Act, 'personal data' encompasses any information pertaining to an identifiable individual[2]. The legislation emphasizes the importance of notice and consent in safeguarding personal data. It outlines obligations for fiduciaries, regulations for processing data of children, and requirements for significant data fiduciaries.[3] The Data Protection Act introduces fines and penalties for breaches of its provisions and associated rules. Similar to data protection laws in other jurisdictions, it possesses extraterritorial jurisdiction, particularly when processing involves Indian data subjects outside India or is connected to activities offering goods or services to individuals within India[4]. Additionally, the legislation addresses aspects such as data transfers, the appointment of data protection officers, and the lawful basis for processing.

Before the enactment of the Data Protection Act, the protection of personal data and privacy concerns fell under the purview of the Information Technology Act, 2000 ("IT Act"), along with relevant rules like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018, and the Intermediaries Guidelines. With the introduction of the Data Protection Act, the SPDI Rules were officially repealed on August 11, 2023.

[1] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023).
[2] *Id.* Section 2(t).
[3] *Id*. Section 4.
[4] *Id*. Chapter VI.

The Indian Computer Emergency Response Team ("CERT-In"), designated as the Government's principal agency for matters related to cybersecurity, has issued directives delineated as the "Cybersecurity Guidelines for Government Entities[5]."

The purview of these guidelines extends to all Ministries, Departments, Secretariats, and Offices explicitly enumerated in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, inclusive of their attached and subordinate offices. Furthermore, it encompasses Government institutions, public sector enterprises, and other Governmental agencies falling under their administrative jurisdiction, collectively referred to as "Government Entities." The primary objective of the Cybersecurity Guidelines for Government Entities is to prescribe and implement prioritized cybersecurity measures and controls within Government organizations, their affiliated entities, and safeguard their cyber infrastructure against prevailing threats.

These Cybersecurity Guidelines for Government Entities serve as a foundational document for both internal and external audit teams, including third-party auditors, enabling them to assess an organization's preparedness against security threats and ascertain its requisites. The guidelines encompass best practices distributed across various security domains, encompassing Network Security, Application Security, Data Security, Auditing, and Third-Party Outsourcing. Acknowledging the dynamic nature of the threat landscape, the Cybersecurity Guidelines for Government Entities are conceived as an adaptable document and will be periodically updated to align with evolving threats.

The implementation of the Cybersecurity Guidelines for Government Entities mandates organizations to designate a Chief Information Security Officer ("CISO") for IT Security, whose details (Point of Contact) are to be provided to CERT-In. It necessitates the formulation of a cybersecurity policy, delineation of roles and responsibilities for the CISO and a dedicated cybersecurity functional team. The CISO is mandated to have an independent cybersecurity team, distinct from IT operations and infrastructure teams. Organizations are further required to conduct comprehensive internal and external audits of their entire Information and Communication Technology (ICT) infrastructure, and based on audit outcomes, deploy suitable security controls. Other stipulations include maintaining an inventory of authorized hardware and software, implementing automated scanning mechanisms to detect unauthorized devices and software, and staying abreast of the latest cybersecurity threats through regular monitoring of CERT-In's website and adherence to associated alerts and advisories.

[5] *Guidelines on Information Security Practices for Government Entities*, Issued by Indian Computer Emergency Response Team (CERT-In) Ministry of Electronics and Information Technology Government of India: Available at https://www.meity.gov.in/writereaddata/files/Guidelines%20on%20Information%20Security%20Practices%20for%20Government%20Entities.pd (Last Visited on 14/01/2024).

The Unique Identification Authority of India ("UIDAI"), operating under the Ministry of Electronics and Information Technology ("Meity"), introduced an advanced security mechanism for Aadhaar-based fingerprint authentication in February 2023[6].

This new security measure employs artificial intelligence (AI) and machine learning (ML) technologies to enhance the robustness of the authentication process and expedite the identification of spoofing attempts.

Developed by UIDAI, this AI and ML-based security mechanism utilizes a combination of finger minutia and finger image analysis to assess the liveness of the captured fingerprint. The implementation of this innovative two-factor/layer authentication introduces an additional verification step, ensuring the authenticity and vitality of the fingerprint and thereby reducing the likelihood of successful spoofing attempts.

This development holds significant implications for various sectors, including banking and financial services, telecommunications, and government entities. Additionally, it is expected to have a positive impact on the broader population, particularly those at the bottom of the socioeconomic pyramid, by reinforcing the Aadhaar-enabled payment system and thwarting illicit efforts by nefarious actors.

In March 2023, the Ministry of Finance issued a notification to bring all transactions involving virtual digital assets ("VDA") under the ambit of the Prevention of Money Laundering Act, 2002 ("PMLA")[7].

This notification empowers the Enforcement Directorate ("ED") to investigate illegal online transactions. Following the issuance of this notification, the ED traced financial transactions involving entities that had illicitly remitted 'proceeds of crime' from India to China and other foreign nations through payment aggregators/enablers and cryptocurrency exchanges. In April 2023, the Indian Parliament disclosed ongoing investigations by the ED into several cases of cryptocurrency/virtual digital currency frauds, implicating certain cryptocurrency exchanges in money laundering activities.

In a parallel development aimed at bolstering the cybersecurity of digital payments, the Reserve Bank of India ("RBI") announced draft regulations for Payment System Operators ("PSO") on 2nd June, 2023. According to the proposed regulations, PSOs are entrusted with defining appropriate 'key risk indicators' to identify potential risk events effectively, along with 'key performance indicators' to assess the efficacy of security controls. The RBI plans to implement these proposed master directions in a phased manner. Specifically, large non-bank

[6] All India Radia, "*UIDAI rolls out new security mechanism for Aadhaar-based fingerprint authentication & faster detection of spoofing attempts*" Available at:< https://newsonair.gov.in/News?title=UIDAI-rolls-out-new-security-mechanism-for-Aadhaar-based-fingerprint-authentication-%26-faster-detection-of-spoofing-attempts&id=456629#:~:text=The%20artificial%20intelligence%20and%20machine,even%20more%20robust%20and%20secure.> (Last Visited on 12/01/2024).

[7] Ministry of Finance, Department of Revenue Finance Intelligence Unit-India (F.No. 9-8/2023/COMO+PL/FIU-IND).

PSOs, Payment Aggregators (PAs), card payment networks, large Prepaid Payment Instrument (PPI) Issuers, non-bank ATM networks, White Label ATM Operators, Clearing Corporation of India Limited (CCIL), National Payments Corporation of India (NPCI), NPCI Bharat Bill Pay Limited, Trade Receivable Discounting System (TREDS), and Bharat Bill Payment Operating Units are required to achieve compliance by 1st April 2024. Medium non-bank PSOs, such as Cross-border (in-bound) money transfer operators under the Money Transfer Service Scheme (MTSS) and Medium PPI Issuers, have an extended timeline until 1st April 2026 for compliance. Small non-bank PSOs, including Small PPI Issuers and Instant Money Transfer Operators, are granted until 1st April 2028 to align with the draft master directions upon their formal enforcement.

In March 2023, the Press Information Bureau ("PIB") officially declared the introduction of the proposed Digital India Act, 2023 ("Digital India Act") as a replacement for the 23-year-old Information Technology Act[8].

On 9th March 2023, a succinct PowerPoint presentation outlining key components of the Digital India Act was disseminated on the website of the Ministry of Electronics and Information Technology ("Meity").

According to this presentation, the envisaged Digital India Act is designed to encompass the principles of Digital India, specifically focusing on Open Internet, Online Safety and Trust, Accountability and Quality of Service, Adjudicatory Mechanism, and New Technologies.

The presentation emphasized the incorporation of a specialized and dedicated adjudicatory mechanism to address online civil and criminal offenses. This mechanism is envisioned to be easily accessible, providing timely remedies to citizens, resolving cyber disputes, fostering the development of a unified cyber jurisprudence, and enforcing the rule of law in the online domain.

In addition to these provisions, the presentation underscored the inclusion of measures ensuring accountability for safeguarding the fundamental rights of citizens as enshrined in Article 14, 19, and 21 of the Constitution of India. The ethical utilization of Artificial Intelligence (AI)-based tools to protect the rights and choices of users, as well as the incorporation of deterrent, effective, proportionate, and dissuasive penalties, were highlighted as salient features of the proposed Digital India Act.

Furthermore, the presentation outlined various types of intermediaries, encompassing e-commerce, digital media, search engines, gaming, AI, over-the-top platforms, telecom service providers, ad-tech, and significant social media intermediaries. It stressed the necessity for distinct rules tailored to each class of intermediaries.

[8] Ministry of Electronics and Information Technology, " *Proposed Digital Act, 2023*" Available at: < https://meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf> (Last Visited on 13/01/2024).

Case Laws:

Intermediaries are obligated to adhere to judicial orders solely on grounds specified within the framework of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("Intermediary Guidelines").

CASE TITLE: WHATSAPP LLC V. UNION OF INDIA[9]

A writ petition invoking Article 226 of the Constitution of India was presented before the Hon'ble High Court of Tripura by WhatsApp. The petition contested the validity of the Intermediary Guidelines and also challenged an order issued by a Judicial Magistrate First Class. The said order directed WhatsApp to disclose the originator of a chat containing a fabricated resignation letter of the Hon'ble Chief Minister of Tripura, citing Rule 4(2) of the Intermediary Guidelines.

The Intermediary Guidelines mandate social media intermediaries to comply with judicial orders. WhatsApp argued that the Guidelines necessitate compliance with judicial orders only under specific circumstances, such as for the prevention, detection, investigation, prosecution, or punishment of offenses related to the sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order, or incitement to an offense. WhatsApp contested the order of the Judicial Magistrate First Class, asserting that the said order failed to establish grounds related to public order or an imminent threat to public order.

The Union of India's ("UOI") submissions before the Hon'ble High Court of Tripura were documented in one of the orders. UOI contended that WhatsApp, as an intermediary, lacks standing to object to the disclosure of the first originator of the message. In a subsequent order dated 27th September 2023, the Hon'ble High Court of Tripura granted interim relief to WhatsApp, staying the order of the Judicial Magistrate First Class seeking the disclosure of the originator. The court determined that the Judicial Magistrate First Class had not addressed the issue of a 'threat to public order' as envisaged under Rule 4(2) of the Intermediary Guidelines.

Constitutional Challenge to CERT-In Directions of 2022

CASE TITLE: SNT HOSTINGS V. UNION OF INDIA[10]

SNT Hostings initiated a writ petition before the Hon'ble Delhi High Court challenging the directives issued by CERT-In on 28th April, 2022 pertaining to Information Security Practices, Procedure, Prevention, Response, and Reporting to Cyber Incidents for Safe and Trusted Internet ("CERT-In Directions"). Specifically, SNT Hostings contested the directions outlined in Paras 4 and 5 of the CERT-In Directions. These particular directives in Paras 4 and 5 pertain to

[9] W.P. (C) 13997 of 2022.
[10] W.P. No. 13170 of 2022.

the mandatory logging of all Information and Communication Technology (ICT) systems and the secure maintenance of these logs for a continuous period of 180 days within the jurisdiction of India. Additionally, service providers, VPN service providers, data centers, etc., are required to register accurate information for a duration of 5 years or more concerning details of customers, among other elements.

SNT Hostings asserted that these directions exceed the powers conferred upon CERT-In under Section 70B(4) of the Information Technology Act. Furthermore, the petitioner contended that the directions lack clarity regarding the nature and extent of the required compliances. Additionally, SNT Hostings challenged the directions based on principles established by the Supreme Court in the case of *Shreya Singhal vs. Union of India*[11]. As of the order dated 17th February 2023, the pleadings in the case are complete, and the matter is currently pending before the Hon'ble High Court of Delhi.

Intermediaries are obligated to mandatorily adhere to blocking orders issued by the Department of Telecommunications (DoT) and the Ministry of Electronics and Information Technology (MeitY).

CASE TITLE: X CORP V. UNION OF INDIA[12]

X Corp. initiated a writ petition under Article 226 of the Constitution of India before the Hon'ble High Court of Karnataka at Bengaluru, challenging MeitY's authority to issue blocking orders with procedural and substantial non-compliance of Section 69A of the IT Act. Among the issues presented before the Hon'ble High Court was the interpretation of Section 69A of the IT Act read with the Website Blocking Rules, specifically addressing whether the power authorizes the direction to block user accounts entirely or is limited to tweet-specific instances. Additionally, the court considered whether the contested blocking orders violate the doctrine of proportionality. X Corp. alleged, among other grounds, that the blocking orders issued by MeitY lacked proper justification, were non-specific, and were disproportionate and excessive. X Corp. further asserted that such orders contravened Article 14, 19, & 21 of the Constitution of India.

The Union of India countered X Corp.'s contentions by asserting that X Corp. is a foreign company, and the claim of fundamental rights violation by a foreign company is not tenable. The Union of India also argued that X Corp., being a non-Indian company, cannot invoke Articles 19 and 21 of the Constitution of India. Moreover, the Union of India contended that the account holders' details are exclusively within X Corp.'s purview, rendering authorities unable to issue notices to them. The Union of India also emphasized that X Corp.'s delayed

[11] [(2015) 5 SCC 1].
[12] 2023 SCC OnLine Del 5094.

compliance with the blocking order resulted in culpable conduct due to the spontaneity and virality of the tweets.

Addressing the issue of the maintainability of X Corp.'s petition under Article 226, the court affirmed the settled position that X Corp. has locus standi under the writ jurisdiction. Concerning the government's power under Section 69A of the IT Act, the court, applying purposive interpretation, held that the power extends to user accounts in their entirety and is not limited to specific tweets. The court found the contested blocking orders to be proportionate. On the matter of non-speaking orders, the court determined that the orders under challenge are speaking orders, demonstrating a substantial nexus between the orders and the assigned reasons. Moreover, these reasons were discussed by MeitY with X Corp. in committee meetings.

Regarding the issue of notice to the user, the court held that, in accordance with the Website Blocking Rules, the absence of notice to the user does not provide grounds for the intermediary to challenge the Blocking Order. The court further ruled that X Corp.'s petition is barred by delay and laches, constituting culpable conduct. Consequently, no relief can be granted in the equitable jurisdiction under Article 226 of the Constitution of India.

Finally, in addressing the issue of culpable conduct and the imposition of exemplary costs, the court noted the extensive pleadings of both the petitioner and respondents. It observed that the subject writ petition, being heard for an extended period, had kept worthier causes of native litigants at bay. The court highlighted the fact that the blocking orders were not implemented by the petitioner for over a year without a plausible explanation. It characterized this as wilful non-compliance, noting the cascading adverse effects of such noncompliance. The court termed the blocking orders' implementation as "abrupt" and "clandestine" with a reservation to challenge, describing it as a case of speculative litigation. Consequently, the petitioner was held liable to bear exemplary costs.

Ultimately, the Hon’ble Court dismissed X Corp.'s petition, imposing a cost of INR 50,00,000 payable to the Karnataka State Legal Services Authority, Bengaluru, within 45 days. Any delay in payment would attract an additional levy of INR 5,000 per day.

Merchants are considered 'third parties,' and no authorization from the Reserve Bank of India (RBI) is required.

CASE TITLE: ABHIJIT MISHRA V. UNION OF INDIA4

Public Interest Litigations were initiated before the Hon’ble High Court of Delhi, seeking appropriate writs, orders, or directions to compel the respondent, Google Pay India Services (P) Ltd., to cease operations in India due to alleged violations of regulatory and privacy norms.

The petitioners contended that Google Pay had breached privacy norms by accessing and utilizing consumers' personal data, including Aadhar details, contravening Section 29, 38(g),

and 38(1) of the Aadhar Act, 2016 ("Aadhar Act"); the Payments and Settlement Systems Act, 2007 ("PSS Act"); and the Banking Regulation Act, 1949. Furthermore, it was argued that Google Pay's operations in India as a payment system provider were unauthorized, as the necessary permissions had not been obtained. Consequently, the storage of sensitive information by Google Pay was deemed an offense under Section 43 of the Aadhar Act.

The petitioners also asserted that, based on the terms and conditions of Google Pay, the application operated on the Unified Payments Interface (UPI) platform, functioning as a facilitator of transactions. Therefore, Google Pay was purportedly acting as a Payments System Provider ("PSP") without proper authorization from the RBI, violating Sections 4 and 7 of the PSS Act, constituting an offense under Section 26 of the PSS Act.

The Hon'ble Court, referring to pertinent sections of the PSS Act, which define 'payment system,' 'system participant,' and 'system provider,' along with Section 7 granting RBI the power to authorize payment systems, held that the National Payments Corporation of India (NPCI) was the operator of the UPI system, authorized by the RBI to extend its services. Transactions through UPI via Google Pay were deemed peer-to-peer or peer-to-merchant and not classified as a system provider under the PSS Act.

The Court further noted that the UPI Guidelines, 2019, clarified the storage of data into 'customer data' and 'customer payments sensitive data.' The latter could only be stored with payment services providers' bank systems and not with third-party apps, as Google Pay had adopted a multi-model API approach. The Court rejected the petitioner's contention that Google Pay actively accessed and collected sensitive user data.

The Hon'ble Court observed that third-party apps like Google Pay were designed to provide a substantial customer base to participating banks. Google Pay received approval from NPCI to operate on the UPI platform, and under the multi-bank application system, NPCI provided a common library for integration to Third-Party App Providers ("TPAPs") on behalf of PSP banks. The Court further opined that the Procedural Guidelines, 2019, clarified UPI models, and under the bank architecture model adopted by Google Pay, transactions were routed through participating banks connected to the NPCI-NET. The RBI, as per its counter affidavit, confirmed that Google Pay was a mere third-party app provider, requiring no authorization from RBI under the provisions of the PSS Act. Consequently, the Hon'ble Court dismissed the petitions.

LEXSPECTRUM'S COMMENT:

In conclusion, the year 2023 has witnessed a technological landscape characterized by rapid advancements and transformative shifts. As society embraces the possibilities offered by information technology, the ongoing journey into the digital frontier promises continued innovation, improved efficiencies, and new paradigms for how we interact with the digital world. All these advancements require regulation, ensuring compliance within the confines of legal parameters.

The legal updates in information technology in 2023 signify a paradigm shift in how Governments approach the regulation of the digital sphere. With a focus on data protection, cybersecurity, emerging technologies like AI and ML, and the regulation of virtual assets, lawmakers are striving to keep pace with the ever-evolving technological landscape. As the year unfolds, it is evident that legal frameworks are becoming more nuanced and adaptive to the challenges and opportunities presented by the digital age.

Practice Area: General Corporate

Authors: Team-Lexspectrum (under guidance of Manish Gaurav, Founder Partner, Lexspectrum and Mr. Akbar Siddique, Associate)

Delhi Office: A-384, First Floor, Defence Colony, Delhi-110024