June 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 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.

Independent Research Institute Calls for New UK Laws on Use of Biometrics

Article Contributed by Aryan Mohindroo (Associate)

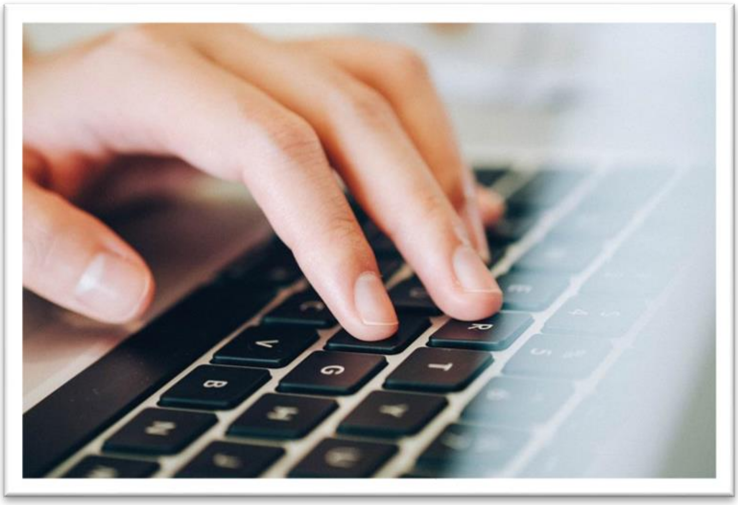
A recent independent review by the Ada Lovelace Institute has revealed that the UK is in urgent need of new laws to govern the use of biometric technologies. The review has called on the UK government to introduce new legislation for their governance. The legal review has provided 10 (ten) recommendations for regulating the use of biometrics by UK investigative agencies. These recommendations include suspension of the public use of live facial recognition technologies until a legally binding code of conduct is established to govern its use. The review also recommends the enactment of a wider, technology-neutral legislation to establish a statutory framework to govern the use of biometrics for law enforcement.

The Ada Lovelace Institute's review has found that biometric data is being used in a growing number of applications in everyday parts of society and everyday lives. This use goes beyond the traditional uses of biometric data in law enforcement and into all areas of citizens' lives.

The hue and cry relating to the unrestricted use of live facial recognition technology by several UK police forces have persisted for long. Around this time last year, even the UK Information Commissioner went public about the unrestricted and reckless use of live facial recognition in public places. Pursuant to such recurrent complaints about the use of the technology, the Information Commissioner's Office ("**ICO**") also fined a controversial U.S. based company Clearview AI, which engages in development of facial recognition technologies. The Company used selfies available on the internet without consent to run an AI based identification matching service. It was ordered to delete UK Citizens' data as well.

RBI Publishes Draft Master Direction on Outsourcing of IT Services

Article Contributed by Smriti Tripathi (Senior Associate)



Regulated Entities ("**REs**") such as banks and NBFCs have been extensively leveraging Information Technology ("**IT**") and IT-enabled services ("**ITeS**") to support their business models and products and services offered to their customers. REs also outsource a substantial portion of their IT activities to third parties. Such reliance on IT/ ITeS provided by third parties exposes the REs to significant risks.

In order to ensure effective management of attendant risks in outsourcing of IT activities, the Reserve Bank of India ("**RBI**") has proposed to prescribe a master direction on outsourcing of IT services to be implemented by the REs. The RBI, on June 23, 2022, published the draft Master Direction on Outsourcing of IT Services ("**Draft MD**") for comments of stakeholders and members of the public, which may be submitted by July 22, 2022. The RBI shall issue the final Master Direction after considering the feedback received from the stakeholders.

The Draft MD has been issued by RBI in the exercise of the powers conferred by Section 35A read with Section 56 of the Banking Regulation Act, 1949, Section 45L of the Reserve Bank of India Act, 1934 and Section 11 of the Credit Information Companies (Regulation) Act, 2005 and provides a risk management framework for the outsourcing of IT Services, managing related concentration risk, its periodic risk assessment and aspects of outsourcing of IT Services to foreign service providers.

In the Draft MD, 'Outsourcing of IT Services' has been defined as an RE's use of a service provider to perform any of the activities listed below on a continuing basis. 'Continuing basis' would include agreements for a limited period. Outsourcing of IT Services mainly covers the following areas but is not limited to:

(a) IT infrastructure management, maintenance and support (hardware/ software/ firmware);
(b) Network and security solutions maintenance (hardware/ software/ firmware);
(c) Application Development, Maintenance and Testing;
(d) Services and operations related to Data Centres;

(e) Cloud Computing Services;
(f) Managed Security Services;
(g) Application Service Providers (ASPs) including ATM Switch ASPs5; and
(h) Management of IT infrastructure and technology services associated with payment system ecosystem.

The provisions of the Master Direction (once finalized) shall be applicable to the following REs: Scheduled Commercial Banks (excluding Regional Rural Banks), Local Area Banks, Small Finance Banks, Payments Banks, Primary (Urban) Co-operative Banks having asset size of ₹1000 crore and above, Non-Banking Financial Companies in Top, Upper and Middle Layers, Credit Information Companies and All India Financial Institutions (NHB, NABARD, SIDBI, EXIM Bank and NaBFID).

The Draft MD provides for the following in detail:

(a) RE's role in outsourcing IT services;
(b) governance framework for approving an IT outsourcing policy and role of the Board and senior management;
(c) evaluation and engagement of service providers by the REs;
(d) provisions to be contained in an outsourcing agreement;
(e) risk management framework to be adopted by the REs;
(f) business continuity plan and disaster recovery plan to be implemented by service providers;
(g) monitoring and control of outsourced activities by the REs;
(h) outsourcing within a group/conglomerate of the RE;
(i) additional requirements for cross-border outsourcing; and
(j) exit strategy enabling the REs to terminate the services of the service provider.

The underlying principle of the Master Direction is that the RE should ensure that outsourcing arrangements neither diminish its ability to fulfill its obligations to customers nor impede effective supervision by the supervising authority. REs desirous of outsourcing IT and IT-enabled services shall not require any approval from RBI. However, such arrangements shall be subject to on-site/ off-site monitoring and inspection/ scrutiny by the supervising authority.

In view of the increasing use of IT/ITeS services by banks/NBFCs and the inevitable need to outsource such services in today's digital world, it is pertinent to put in place a framework around outsourcing of IT services by banks/NBFCs. As such, publishing of the draft master directions by the RBI is a welcome step. Once finalized, the master directions will go a long way in ensuring that banks/NBFCs can provide fast, reliable and efficient service to the customers while at the same time managing/containing the risks associated with outsourcing IT services to third parties.

The draft MD may be accessed here.

‘Intermediaries are Duty Bound to Regulate Content’ – Madras High Court Observes

Article Contributed by Niharika Sharma (Associate)

By an order dated June 7, 2022 passed in *State represented by the Inspector of Police v. A. Duraimurugan Pandiyan Sattai* (‘Decision’), the Madurai Bench of Madras High Court (‘Court’) analyzed the liabilities and obligations of intermediaries, and observed that the intermediaries are obligated to regulate content over the internet.

Brief facts

In this case, the Court was examining a petition filed by a police official under Section 439(2)(3) of the Code of Criminal Procedure, 1973 (‘Cr.P.C’) seeking cancellation of bail granted to one A. Duraimurugan Pandiyan Sattai, for posting offensive videos over ‘YouTube’ with certain derogatory remarks against various persons including the former Chief Minister of Tamil Nadu.

Even though the aforesaid petition was filed under the provisions of Cr.P.C, the Court delved into the provisions of Sections 69A, 79(3)(b) and 84B of the Information and Technology Act, 2001 (‘IT Act’), and noted that whenever a request for blocking content is made by the Central Government/ its officials or as per the community guidelines framed by each intermediary, it is the liability of such intermediary to block content for public access.

Findings of the Court

While allowing the petition for cancellation of bail to Mr. Sattai, the Court observed that Sections 69A, 79(3)(b) and 84B of the IT Act impose certain duties and liabilities on the intermediaries. In addition to this, various intermediaries have framed their respective community guidelines for the regulation of content on social media, in this case, ‘The YouTube Community Guidelines’. Having framed guidelines for its users, it is the duty of the intermediaries to remove or block the channel of any such violator.

The Court further observed that ‘*it is the duty of intermediaries to ascertain whether those videos are in accordance with their policies and guidelines and in terms of the contract and to* *block the channels if the videos are not in accordance with the terms and policies. The intermediaries are not expected to insist for FIR or any court orders to remove the videos which are in violation of their guidelines. If it is not blocked or removed even after it was brought to their knowledge, the intermediaries are committing the offence under Section 69A (3) of the Information Technology Act*'.

The Court sought a reply from the Tamil Nadu government as to whether social media companies can be included as an accused or an abettor in criminal cases involving social media platforms. The Court also asked if the government had any mechanism through which such misuse could be prevented and appointed advocate KK Ramakrishnan as amicus curiae to assist the Court on the issue.

Analysis

The Decision makes certain sweeping observations which have once again brought intermediaries under the spotlight. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 ('IT Rules') are already under the scrutiny of the Supreme Court and on June 6, 2022, the Central Government had invited public comments and consultation from stakeholders on the proposed amendments to the IT Rules which, *inter alia*, require significant social media intermediaries to remove from the internet any content which is obscene, pornographic, invasive of bodily privacy and racially or ethnically objectionable, within 72 hours, as opposed to the current 15 days.

It remains to be seen how an appellate court would react if the Decision is appealed against.

Proposed Amendments to IT Rules, 2021

Article Contributed by Akshay Bhatia (Associate)

On June 6, 2022, the Ministry of Electronics and Information Technology ("**MeitY**"), proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules, 2021**") to '*address challenges and gaps*' that exist in the IT Rules vis-a-vis Big Tech platforms ("**Proposed Amendments**").

These Proposed Amendments are part of the pre-legislative consultation process and have been uploaded on MeitY's website for public feedback and input from all stakeholders for a period of 30 days from the date of publication.

The Proposed Amendments entail the following:

1. **Creation of a 'Grievance Appellate Committee'**: MeitY aims to create Grievance Appellate Committee(s) ("**GAC**") by introducing Rule 3(3), IT Rules, 2021. A GAC shall serve as an appellate to whom appeals shall lie from an order made by the grievance officer ("**GO**") under Rule 3(2)(a) and (b), IT Rules, 2021 within 30 days from the receipt of the communication from such GO. It is proposed that such GAC shall aim to dispose of an appeal within 30 working days from the receipt of the appeal and once an order is passed by the GAC passed, such shall be complied by the concerned intermediary. The rationale given for such setting up of such a GAC is that it provides users an alternative to file an appeal against the order of a GO instead of approaching judicial remedy by way of a court of law. It has also been stated that judicial remedy shall be open to a user at any time against any order of an intermediary or a GO.
2. **Ensuring compliance with Rule 3(1)(b) by intermediaries**: Rule 3(1)(b), IT Rules 2021 requires intermediaries to inform their users, through privacy policies, rules and agreements etc. not to post content that is 'defamatory', 'harmful to child, 'deceiving or misleading', 'in violation of any law' etc. At present, an intermediary is not mandated to remove content falling under Rule 3(1)(b), IT Rules 2021 in the absence of a complaint by a user. The Proposed Amendments, by amending Rule 3(1)(a) and (b), IT Rules, 2021 aim to mandate the removal of objectionable content falling under Rule 3(1)(b), IT Rules 2021 by the intermediary itself, even in the absence of a complaint

by a user. This shifts the burden of compliance on the intermediary, might be difficult to implement and may result in arbitrary and uneven enforcement.

3. **Grievance Redressal within 72 hours**: The Proposed Amendments, by adding two provisos to Rule 3(2), IT Rules, 2021 requires an intermediary, through its GO, to action and redress a complaint for removal of content within 72 hours of the request being made. The rationale given for this is that by the very nature of the internet and its ensuing outreach, pace and virality, content removal complaints should be redressed in a timely manner. It also states that intermediaries may develop safeguards to avoid the misuse of the redressal system by users that submit inappropriate, trivial or inauthentic complaints.
4. **Respect to constitutional rights**: Through Rule 3(1)(m) and (n) of the Proposed Amendments, MeitY requires an intermediary to respect the constitutional rights accorded to the citizens of India under the Constitution. It also requires intermediaries to take reasonable measures to ensure accessibility of its services to all users and to ensure users have a reasonable expectation of due diligence, privacy and transparency.

The Proposed Amendments may increase the burden of compliance on intermediaries. According to compliance reports, Facebook[1] already removes/ takes down around 3 crore pieces of content on a monthly basis in India. The widened scope of objectionable content and increased burden of ensuring compliance even in the absence of a user complaint would require intermediaries to dedicate more resources and be vary of running afoul of the IT Rules, 2021. The introduction of the GAC to hear appeals from orders of the GOs may result in undue governmental interference in freedom of speech accorded under Article 19 of the Constitution and may result in censorship firstly by the intermediaries and then by the GAC, which is constituted by the central government.

The IT Rules, 2021, since their very implementation, have been the subject of litigation before various high courts around the country. Notably, the Bombay High Court and the Madras High Court have stayed Part III, IT Rules, 2021 on the grounds that they are violative of the right to speech and are beyond the rule making powers of the central government, while the Kerala High Court has also passed interim orders stating that no coercive steps shall be taken under the IT Rules, 2021 while the matter is pending before the court. The Supreme Court of India, hearing appeals from orders of various high courts, has stayed said proceedings before the high courts and agreed to hear challenges to IT Rules, 2021 cumulatively on July 19, 2022.

[1] https://drive.google.com/file/d/1zzTt0FJBw-bsnx8QqohdES79s5OntuKT/view

Proposed Changes to UK’s Data Protection Regime

Article Contributed by Anushkaa Shekhar (Associate)

The UK first indicated its intention to overhaul its data protection regime when it published its new National Data Strategy on September 9, 2020, nearly eight months after the Brexit Withdrawal Agreement came into force and the transition period began. The 11-month transition period ended on December 31, 2020 and the UK formally and effectively left the EU on January 1, 2021. On this date, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations, 2019 came into force which called for a domestication of the EU General Data Protection Regulation (**“EU GDPR”**). The UK then introduced the UK GDPR, which combined the two previously existing regimes for personal data protection, notably the EU GDPR and the Data Protection Act, 2018. At this point, the UK GDPR was a replica of the EU GDPR and was amended only to substitute some parts of the text from ‘EU and Union law’ to ‘UK and domestic law’.

But when the Department for Digital Culture, Media & Sport published its consultation on proposed reforms to the UK’s data protection regime (the “**Consultation**”) on September 10, 2021, it constituted a major departure from current UK legislation and the EU GDPR. This significant shift was described as ‘a clampdown on bureaucracy, red tape and pointless paperwork’ that comes along with the EU data protection law. Responses to the consultations were accepted for a period of 10 weeks till November 19, 2021. The response to the Consultation (**“Draft Proposal”**) was released on June 17, 2022. The voluminous document is the result of approximately 3,000 public replies and more than 40 roundtable discussions with stakeholders from academics, technology, and industry, as well as consumer rights groups. Some of the major reforms that are in the offing are:

1. **Introduction of Privacy Management Programmes (“PMP”)**
   Key components of the current accountability system are to be replaced by a more adaptable, risk-based Privacy Management Programme. The programme’s comprehensiveness will be determined by the volume and sensitivity of personal data handled by an organization.

1.1. The PMP approach would be based on a number of elements at the core of accountability, such as:

- leadership and oversight
- risk assessment
- policies and processes
- transparency
- training and awareness of staff
- monitoring, evaluation and improvement

1.2. To support the implementation of PMPs, the government has proposed the removal of certain requirements under the UK GDPR:

- Removal of Data Protection Officers (**"DPO"**): The post of DPOs, whose role was to oversee the organization's data protection strategy, has been done away. Instead, appointment of a suitable senior individual who will be responsible for the PMP is envisaged. The role has not yet been fully particularised, but it seems likely to be less formal than that of DPO and without the independence requirements.
- Removal of Data Protection Impact Assessments (**"DPIA"**): Organizations will no longer be required to undertake DPIA. Rather, the Draft Proposal stipulates implementation of risk assessment tools which help assess, identify and mitigate risks.
- Relaxation under Article 30: Lastly, the Draft Proposal has removed the requirement to keep a record of processing activities based on Article 30 of the EU GDPR. The organizations have been given more flexibility in their record keeping requirement.

2. Placing cookies without user's consent

Under current regulations, cookies are not permitted to be placed on a device without the user's consent, which is usually sought through a pop-up notice. However, now the government intends to permit cookies to be placed on a user's device without explicit consent, for some non-intrusive purposes, like audience measurement cookies. Gradually, the government aims to switch to an opt-out model of consent for website cookies. This means that cookies can be set without the user's knowledge, but the website will have to provide explicit instructions on how to opt out. However, the opt-out model would not apply to websites likely to be accessed by children.

3. Change in the functioning of Information Commissioner's Office ("ICO")

Under the EU GDPR, ICO is the independent regulatory office in charge of upholding information rights in the interest of the public. However, as per the Draft Proposal, the secretary of state will now set out a statement of strategic priorities for the ICO, which will first have to be approved by parliament. The ICO will be required to respond to these priorities but will not be legally bound to act in accordance with the statement. The ICO's governance will also be reformed and it will be renamed.

4. Change in threshold for subject access request

The current regime provides for subject access requests, which means that the individuals have the right to access and obtain a copy of their personal data, as well as other related information from an organization. The organizations have the right to deny subject access request if they deem the request to be 'manifestly unfounded or excessive'. The Draft Proposal aims to change this to threshold to 'vexatious or excessive'.

These proposed reforms are likely to form the basis of the forthcoming UK Data Reform Bill. While the aim of the government was to simplify the data protection regime by bringing in these reforms, it may actually make things difficult for UK based companies. When selling goods and services to the EU, enterprises situated in the UK will have to follow EU data privacy regulations. As a result, many businesses may not benefit from the simpler legislation that is being proposed for the UK and will have to juggle a dual track regime.

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:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com

Key Contacts for the Data Privacy and Technology Practice

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

Udit Mendiratta, Partner
udit.mendiratta@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