March | 2022 Discussion Paper

CUTS International
www.cuts-international.org

Impact of Criminalising Provisions on Ease of Doing Digital Business in India

Neelanjana Sharma, Senior Research Associate, CUTS International

Overview

In the Ease of Doing Digital Business (EoDDB) Study course, the researchers have taken up a discussion paper series on various topics that impact Digital Businesses in India. This Paper will discuss the aim of India's Digital First Economy and the role of Digital Businesses in its realisation.

The paper will introduce the Ease of Doing Business (EoDB) reforms undertaken by the Government of India, emphasising decriminalisation of regulations to enhance EoDB. Further, it explains criminalising provisions and tries to decode them for digital businesses in India. While decoding the criminal provisions, the paper covers regulations containing the imprisonment provisions and their use in judicial cases. It also discusses Brazil's civil liability framework for intermediaries along with other best practices across some countries. In conclusion, the paper tries to elaborate upon the way forward while suggesting some recommendations for the future of criminal liability of digital businesses in India.

Introduction

India aims to be a digital-first economy and seeks to create an economic value of US$1tn from its digital economy by 2025, as per a report[1] by the Ministry of Electronics and Information Technology (MeitY). For the digital economy and businesses to flourish, a regulatory environment and ecosystem that enables such growth must be fostered, assisting India's EoDDB. One of the key aspects that impact businesses, traditional or digital, is the country's regulatory environment.

Over the past decade, India has made substantial progress towards EoDB reforms. One of the key steps taken was removing criminalising provisions from several regulations and laws, which encouraged innovation and increased the entrepreneurial spirit of the youth. However, this non-criminalising touch of the government remains aloof from the businesses that have digital at their core or which exist digitally alone and deal with consumers' data.

Rapid digitalisation has turned out to be a double-edged sword for the government. It has opened up the markets for innovation and has increased access to information, goods and services in India. However, it has also accelerated regulation development on a still young landscape. Regulations are not always of the nature to promote the EoDDB.

In this paper, the parallels between the regulatory intentions towards digital and traditional businesses from the lens of criminalising provisions and their usefulness are brought to light. This paper aims to initiate a discourse on the gap between traditional and digital businesses and their regulatory environment in India. With the acceptance and encouragement of EoDB, India should also cater to EoDDB to achieve its goal of a digital-first economy. This paper will attempt to reveal the hindrances caused by criminal penalties; later will decipher alternate mechanisms which can

be used to avoid such hindrances while fulfilling the objectives of such provisions.

Criminal Liability of Businesses

The traditional starting point of criminalisation is the 'harm principle' where John Stuart Mill stated that the only purpose for which power can be rightly exercised over the members of a civilised society against their will is to prevent harm to others.[2] The number of laws targeted towards digital businesses are not infinite but more than those required.

The rule of criminal liability stands upon the maxim 'actus non facit reum nisi mens sit rea means', which can be loosely translated into that the Act is not wrongful unless it is done with a wrongful state of mind.

Though the corporation is a separate legal entity and can therefore commit a crime, the criminality principle cannot be exercised in isolation from the principle of proportionality. The principle of proportionality states that there needs to be a reasonable nexus between the desired results and measures taken to reach that goal.[3]

Criminal penalties in business mean terms of imprisonment for certain actions. The existence of criminal provisions for procedural, structural or minor offences suggest that violation of rules and non-compliances are offences of serious nature that require imprisonment as part of the punishment. As the criminal offence accompanies mens rea (mental intention);[4] the applicability of such jurisprudence to digital businesses seems at variance from traditional businesses.

Also, criminal penalties of imprisonment need to be viewed on its usefulness and effectiveness. One of the criticisms faced by the opposition of imprisonment clauses is that the provisions are hardly ever used. However, if the provisions are not used, their necessity should be taken on merit as a useless law weakens the necessary law. The distinction between what is necessary and what is useless perpetuates fear and questions the lawmaker's intent, which ends up criminalising entrepreneurship and business entities.[5]

The offences would be dealt with by the adjudication officer of the IAM Framework, who would be able to determine penalties through order, the appeal of which would lie with regional directors.

Decriminalisation under EoDB

Due to pandemic India's EoDB framework streamlining has been pushed to the forefront and follows three steps: rationalising, digitising and decriminalising.[6] One of the key aspects of those reforms has been decriminalising various technical and procedural provisions. After extensive analysis, more than three hundred low risk offences have been decriminalised.[7] Below mentioned are some of the laws which were altered to keep up with the EoDB provisions:

The Companies' Act, 2013

In light of the pandemic, companies faced difficulties in keeping up with the regulatory and procedural aspects of the Companies Act 2013. The Government of India (GoI) had decriminalised certain provisions that contained compoundable offences to adapt to the changes. This was done keeping in mind the EoDB and promoting foreign investment. This will also encourage young entrepreneurs to start their businesses in India instead of seeking foreign jurisdictions and markets.

The 23 offences of minor nature, such as non-compliance, were reclassified and moved to In-House Adjudication Mechanisms (IAM) Framework as they were the offences that could be dealt with objectively.

Other than 23 offences, seven offences capable of being dealt with using other laws were excluded from the Companies Act. Furthermore, 11 offences that were not of grave violation and compoundable were restricted to the imposition of fine only as they involved subjective determination. The Company Law Committee (CLC) had recommended the creation of alternate mechanisms to impose a sanction and that recommendation was accepted as is by the GoI.[8]

The Limited Liability Partnership Act, 2008 (LLP Act)

After the Companies Act, to make LLPs feel like an interesting and safe option and encourage EoDB, GOI had approved decriminalising 12 provisions out of the total 24 provisions that were penalising in nature.[9]

India has over two lakh LLPs and in the past financial year, there has been a 17 percent growth in the number of LLPs incorporated in India. The amendment boosted the inclination towards LLPs and contributed towards EoDB.

To decriminalise the offences two major steps have been taken. Firstly, there has been the reduction of penalties for several compoundable offences and some of the offences of minor nature have been moved to IAM Framework.

In furtherance of the offences being punishable with fines, the regional directors can compound those offences. The scope of the section has been broadened to include the process of compounding of offences by the regional directors.[10]

Other Miscellaneous Measures for Decriminalisation

The Department of Financial Services, Ministry of Finance had also initiated a process by inviting public comments to decriminalise minor offences under 19 acts and financial laws for improving business sentiment and unclogging court processes.[11]

In view of the measures of decriminalisation undertaken by the GOI have given the strength to single businesses such as brand retailers to ask for decriminalisation of *The Legal Meteorological Act, 2009.*[12] Under this Act, 23 provisions have imprisonment provisions for offences of compoundable and non-compoundable nature. The retail businesses representatives claimed that the Act is archaic and involves imprisonment as punishment for offences that might be caused due to an oversight. GoI will soon finalise decriminalisation of offences on similar grounds as was done under the companies act and the LLP act.

Decoding the Criminalising Provisions for Digital Businesses

The advent of digital technology in all businesses is evident and even traditional businesses have some digital component in them. Rapid digitalisation has opened markets of innovations and increased access to goods and services, but it has also created a burden on the young regulatory landscape of the country.

This is exactly what intermediary liability

Intermediary liability means that the intermediary is held liable for everything his users do -Rebecca MacKinnon.

entails for service providers in India. As elaborated above, corporate law jurisprudence in India is moving away from criminal liabilities towards civil sanctions. However, in the past decade, multiple regulations have been

formulated which directly impact digital businesses. A few proposed and existing laws paradoxically mandate provisions that impose certain criminal penalties on digital businesses.

Such laws and regulations hinder investment decisions and make it challenging to do digital business. They could also convey contradictory approaches to the GoI's aim and objective to enhance EoDB in India.

Information Technology Act, 2000 (IT Act) and Rules thereunder

Under the definition of intermediaries, thus, digital businesses, which are social media companies, search engines, digital payment service providers, amongst others, are included. Therefore, any provision applicable to an intermediary would apply to these digital businesses, including provisions containing imprisonment clauses.

IT Act provides safe harbour provisions where Section 79[13] protects social media intermediaries against legal action for any third-party information, data, or communication link made available or hosted by it. However, this protection only applies if the said intermediary does not initiate the transmission of the message in question, select the receiver of the transmitted message, and do not modify any information contained in the transmission.[14]

Section 79 and associated rules introduced to protect intermediaries for liability from user-generated content and ensure the internet continues to evolve as a "marketplace of ideas". But as intermediaries may not have sufficient legal competence or resources to deliberate on the legality of an expression, they may end up erring on the side of caution and takedown lawful expression.[15]

Under the IT Act, Section 2(w) defines an intermediary as any person who on behalf of another receives, stores, transmits, records and provides services in respect of this record. It includes service providers of network, telecom, internet, web-hosting, search engines, amongst others.

Below are the sections explained through the case laws about their use and misuse of imprisonment clauses despite the Section 79 provision of safe harbour.

Section 67

Section 67 of the IT Act often includes managing directors and employees of any digital business. The punishment provided under the section consists of fines and imprisonment ranging from three to five years. After the strike down of Section 66 A of the IT Act owing to its rampant abuse, Section 67 is being actively misused to file complaints of cyber defamation.[16]

The CEO of an E-commerce portal was arrested under Section 67 later allowed bail because of an obscene video placed on the website. The CEO had to prove his due diligence.[17] However, the case was registered only for the CEO in this matter. The persons who uploaded the objectionable material remained unidentified, thus making the CEO liable for third-party action.

Recently, the managing director of Alt Balaji (a digital media streaming business) was charged with multiple FIRs (Hyderabad, Madhya Pradesh (MP), Delhi) for publishing obscene material and hurting complainants' religious feelings. It is important to note that MP FIR was registered by name and did not include the business' name. The managing director was neither the producer nor the show's director and was not credited in the episode.[18]

The FIR of the Delhi and Hyderabad case was later dismissed due to a lack of evidence in the case.[19] However, the MP High Court refused to quash the case,[20] and accepted that it can be presumed that a managing director having no part in conceptualising, publishing, directing and producing would have known the contents

of each episode. The onus of proving otherwise was shifted to the managing director for proving, by way of evidence, that she did not possess such knowledge. Though the managing director issued a public apology and the scene in question was deleted without it requiring a direction from court, the managing director had to move the Supreme Court for interim protection from arrest.[21]

Through this scenario, one thing that can be implied is, the persons who created the episodes, the users who paid for the subscription and watched the episodes faced no criminal charges, however, a managing director with no criminal intent faced multiple FIRs.

Section 69 and Rules Thereunder

Under Section 69 of the IT act, Intermediaries are required to provide technical assistance and facilities for providing or securing access, intercept, monitor or decrypt and provide information stored in computer resources.

Intermediary in contravention with Section 69 and rules thereunder is liable to be punished with imprisonment up to seven years.

The procedure for the interception, monitoring and decryption is provided for in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (2009 rules),[22] which are to be read with Section 69 (2) of the IT act. Under Rule 21 of the rules mentioned above, it is stated that intermediaries can be held liable for any action of their employees and can be made liable under any law for the time being in force.[23]

In a 2022 case,[24] The appellant had filed an RTI to seek statistical data about Section 69, which was denied. In this appeal, the appellant also presented as evidence the pleadings of five petitions (pending before the Supreme Court) which challenged the constitutional validity of part of section 69, Section 5(2) of the Telegraph Act, 1885 and rule 4 of the rules made under Section 69 B on the grounds of legislation not satisfying the test of proportionality put forth by the right to privacy judgement by the Supreme Court.[25]

The court adjudicated that, materials are retained for more than the prescribed period due to an overlap exemption under the rules. There is no reason for not providing the information sought under the Right to Information Act, 2005. However, some guidelines were prescribed for the duration for which data can be retained under every order and rules.

In between the challenges on validity scope of rule-making power of the provisions, one thing that remains intact and untouched is an intermediary liability. In India, the approach followed for intermediary liability is vertical in design, wherein different liability regimes under various statutes apply to intermediaries.[26]

Section 85

Section 85 of the IT Act makes the director and every person who was in charge and responsible for the conduct of the business at the time of the contravention liable to be proceeded against and punished. The section provides for an exemption from this liability in case the person is able to prove his due diligence which was then used by the CEO of Bazee.Com.

In a Delhi High Court Case, where profile pictures of the petitioner were taken from social media websites and uploaded on pornographic websites, no claim was sought by the petitioner from the social media websites.[27] However, in another case, the social media companies were directed to remove any other material the plaintiff may report as objectionable.[28]

The exemption provided under Section 85 and Section 79, however, seems infructuous after the release of Information Technology

(Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[29] (Intermediary Rules, 2021)

The above-stated provisions are the most commonly used imprisoning provisions. However, there are other provisions with imprisonment clauses that have the potential to be misused. The same is provided below.

Section 67 C and Rules Thereunder

Section 67C of the IT act if an intermediary intentionally or knowingly fails to preserve or retain information for a prescribed duration, manner and format for central government, then such intermediary shall be liable to be punished with imprisonment up to *three years*. GOI released the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.[30] Though the rules do not contain any provisions for imprisonment, they do place a compliance burden on intermediaries.

Under these rules, Intermediaries, internet service providers, websites, apps like Facebook, WhatsApp and Gmail are required to collect and store data. Data retention laws can quickly become a 'legal' means of violating people's fundamental right to privacy without the necessary safeguards.[31]

In case of infringement of the rules and Section 67 C, without taking it on a case-to-case basis or keeping a scope of communication of inability to comply with the law, the first step undertaken is imprisonment. It needs to be reiterated for the whole of IT Act that though well-intentioned, one of the major gaps in the implementation of the IT Act is that it wades into criminal liability straightaway. The case is not always wilful illegality, wherein a crime may have been committed but may not be intentional. It is not necessary to convict when penalising can achieve the goal.[32]

Section 69 A and Rules Thereunder

Under Section 69A of the IT Act, Intermediaries can be directed to block public access by way of direction under written orders. In case an intermediary fails to comply with the direction, they can be punished with imprisonment up to *seven years*. Even though the constitutional validity of Section 69A has already been examined by the Supreme Court,[33] where the court noted that the section has been narrowly drafted and provides safeguards. However, it appears that such safeguards are not followed in practice, thus, making intermediaries criminally liable in case of non-compliance.[34]

Under Section 69 A, the GOI had framed the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules)[35] to lay down the rules regarding blocking of information to the public under the information of technology act as some of the confidential information cannot be disclosed.[36]

The government used these rules and section 69A to restrict access to accounts, sites, and networks multiple times, such as Chinese App ban, Twitter accounts, and tweets from certain accounts withheld.[37]

A writ petition was filed inter alia against search engine operators including Google, Yahoo and Microsoft, to hold them liable for displaying advertisements or searches in violation of the Prenatal Sex Determination Act, and the Court imposed obligations to monitor the complaints and respond to complaints relating to the Act upon the search engines.

Even though the Blocking Rules exist and so does section 69A, recently, the Indian Supreme Court has held search engines, liable, as intermediaries, for hosting advertisements and keywords relating to pre-natal sex

determination.[38] Court ordered actions for content restriction are outside of any explicit statutory authority, even though similar outcomes may be achieved through existing legislation, such as the Blocking Rules.[39]

Section 69 B

Under Section 69B of the IT act, Intermediaries are required to provide technical assistance and facilities for monitoring and collecting traffic data or information through any computer resource. Intermediaries in the contravention are liable to be punished with imprisonment up to *three years*.

Though the provision in itself seems straightforward, the 2009 Rules are also in convergence with this. On a closer look, Section 69 B empowers the Central Government to authorise any government agency to monitor and collect traffic data or information through any computer resource for cyber security. This sets the stage for direct Internet and internet metadata surveillance, respectively.[40]

Metadata includes internet usage and telephone data, such as time and duration of telephone calls, IP addresses, IDs of senders and receivers of e-mails, log-in and log-off times for e-mail use, etc. Such data excludes the actual content of the e-mails or the messages. While governments argue that metadata does not reveal the individual's personal details, this is not true. An individual's entire internet history can be traced out using just the metadata.[41] This nature of surveillance is dangerous as India currently does not have any Surveillance Reforms in place to protect citizens' privacy.

Section 87 and the Intermediary Rules, 2021 Thereunder

The intermediaries that can be held criminally liable are employees of digital businesses in this case which are specifically employed for compliance and operational purposes, such as compliance officers, directors and nodal officers as was made clear under the Intermediary Rules, 2021.

Further, the Intermediary Rules, 2021, prescribe guidelines for due diligence and grievance redressal mechanism for intermediaries and code of ethics, procedure and safeguards for digital media. In doing so, the rules categorise intermediaries into two distinct categories. Firstly, social media intermediaries primarily enable online interaction between users, allowing them to create, upload, share, disseminate, modify or access information using the intermediary's services.[42]

Secondly, significant social media intermediaries have a number of registered users as notified by the central government, which was later clarified to be at 50 lakh users.[43] These intermediaries would mean businesses such as search engines, internet service providers (ISPs), digital platforms, etc.[44]

These offences directed towards intermediaries have requirements of complying with directions failing which the first step undertaken is imprisonment. There is a space between these two actions to show-cause notices, seek clarification on non-compliance etc.

Under the Intermediary Rules, SSMIs are required to appoint a chief compliance officer (CCO)[45], a nodal contact officer[46] and a resident grievance officer[47], all must be residents of India. The chief compliance officer is responsible for ensuring compliance with the IT Act and Rules, and will be held liable in any proceedings in instances[48] of non-compliance with the IT Act and Intermediary Rules.[49] Similar penalising provisions for non-compliance by other intermediaries are given under Rule 7 of Intermediary Rules.

The appointment of CCO was not without its troubles. The businesses were sceptical about the liabilities attached to the role. Experts

suggested that the CCO be responsible for all compliance requirements and non-compliance shall entail jail term. According to Rule 7, non-observance of Rules may take away of the protection of Section 79 of IT Act and non-observance shall be punishable under any law, including IPC (Indian Penal Code) where criminal charges can be determined and sentence for jail is also possible for the CCO as per Rule 4(1) (a).[50] Also, the Intermediary Rules, 2021 provide for the CCO to be a key managerial person of the company, which can be the CEO or the MD, Chief Financial Officer (CFO), Manager, company Secretary or Whole Time Director.[51] This not only takes away the freedom of the businesses but also comes under the light of over-regulation.

Recently, in a series of First Information Report (FIRs) filed against Twitter, one of the executives in a statement to media questioned if someone will take a job if it came with a caveat of going to jail for a third party's tweet. Similarly, in one of the FIRs filed against Twitter related to the company misrepresenting India by not showing Jammu & Kashmir and Ladakh as outside India, the Managing Director and Twitter India's head of News Partnerships were named in the FIR, even though neither was directly involved in the process of making the maps.[52] The impact of these FIRs on the business can be evaluated from the update that the Managing Director was moved outside India and later ended up quitting Twitter entirely.[53] The automatic attachment of criminal intent with the position of a compliance officer is not only disproportionate but also a deterrent to businesses.

Also, one of the challenges to intermediary protection has been the use of platforms in criminal activities.[54] MeitY has taken up the issue on two separate occasions with WhatsApp and has indicated that if the intermediary does not find a solution for the same, they're 'liable to be treated as abettors' and 'face consequent legal action', which can mean that intermediaries are prosecuted as abettors under the Indian Penal Code (IPC).[55]

Here, there is a lack of clarity on which provisions from the IPC may apply in case of non-compliance and thus, the number of years of imprisonment may be varied for different kinds of non-compliances. This does not find mention in the Intermediary Rules.

The MeitY, in October 2021, had issued FAQs on the Intermediary Rules, to provide clarity and explain the nuances of due diligence to be followed by intermediaries.[56] Further, according to media reports, GoI is also considering amendments to the IT Act to bring in new penalties, such as fines, for social media companies and individuals and retain some of the law's criminal provisions.[57]

These rules have overtaken the Intermediary Guidelines, 2011, against which a petition was filed by MouthShut.com seeking their quashing because they are violative of Article 12, 19 and 21 of the Constitution of India.[58] In the past 10 years, not much has changed except new and more ways have made their way into laws to make intermediaries liable and to violate fundamental rights using the means of regulations.

Payment and Settlement Systems Act, 2007 (PSSA)

The PSSA provides for regulation and supervision of payments systems in India. Section 26(1) of the PSSA prescribes penalties to those who operate without authorisation[59] from the Reserve Bank of India (RBI)[60]. The penalty of imprisonment from 1 month to 10 years has to be judged based on the severity of this punishment which is on two extremes. The penalty of 10 years under the IPC is prescribed

Although the provision is technical and procedural, Section 26(1) prescribes a penalty of imprisonment ranging from as little as one month to as extreme as 10 years or fines or both.

for offences of heinous nature, and anything below seven years of imprisonment is considered a serious offence.[61]

Out of the few provisions of the IPC which have prescribed the 10-year imprisonment, one is the offence of Culpable Homicide not amounting to Murder[62] punishable under Section 304.[63] Even this provision has an addition of 'may extend to 10 years.' It can be deduced that offences under PSSA Act are considered as grave as section 299 of IPC and as frivolous as one-month imprisonment. This will create unnecessary fear in the businesses and the need for such provision thus should be examined on its merit by the regulators.

Also, previously, the Ministry of Finance had called for comments on decriminalisation of thirty-nine minor economic offences, including Section 26(1) and 26(4) of the PSSA to facilitate ease of doing business in India.[64]

The regulator had identified some principles which directly relate to reclassification of criminal offences to compoundable offences such that they would lead to the following results:

a. Decrease the burden on businesses and inspire condense amongst investors;
b. focus on economic growth, public interest and national security should remain paramount;
c. mens rea or criminal intent plays a vital role in the imposition of criminal liability. Therefore, it is critical to evaluate the nature of non-compliance i.e., fraud as compared to inadvertent omission; and
d. the habitual nature of non-compliance.[65]

However, nothing came out from the finance ministry's move as there were no further updates on this action.

Joint Parliamentary Committee's Report on Personal Data Protection Bill, 2019 and Draft Data Protection Bill, 2021 thereunder

In addition to the above regulations, the recent recommendations by the Joint Parliamentary Committee (JPC) on the Draft Data Protection Bill, 2021 (DP Bill, 2021), suggested that social media companies that are not intermediaries or do not act as intermediaries should be treated like publishers.[66] JPC's recommendation to term social media platforms is flawed on the grounds established in *Shreya Singhal Case*[67] , which struck down Section 66A[68] of the IT Act on online free speech and intermediary liability.

Suppose social media companies are termed as publishers and made accountable for any content they hold. In that case, it takes away the safe harbour provisions brought in effect in the 2008 amendment of the IT Act after the Delhi High Court decision in *Avinash Bajaj Case*.[69] It is implied that social media companies will start to pre-screen the content uploaded by the users to keep themselves safe from any liability, which would curtail Article 19(a).[70]

This would give the power of censorship to private entities and take away the freedom of speech and expression outside the reasonable restriction of Article 19(2), which can be imposed only by the state as defined under Article 12 of the Constitution.[71] Though the law is still to be brought in effect, this implication brings liabilities both of fine and imprisonment, which print and online publishers are subjected to under various laws.

Section 83(1) of DP Bill, 2021 states that whoever, without the consent of data fiduciary or processor, knowingly or intentionally re-identifies the data is liable to be punished with imprisonment of up to *three years*. Along with this, Section 85 of DP Bill, 2021 states that any company found in contravention of the Act, person in charge of that part of businesses conduct can be made liable and punished accordingly. Though, DP Bill, 2021's Section 83's call for imprisonment is against the use of personal data, which is justified in the right to privacy.

However, Section 85 of the DP Bill, 2021

mirrors in intention with Section 85 of the IT Act and places unnecessary burden on private data fiduciaries as opposed to government and its agencies who can be given blanket exemption under Section 35 of the proposed bill. If the bill sees the light of the day without any changes, this section might be susceptible to misuse, and experts have not caught up on it yet.

Copyright Act, 1957

The copyright act went through some amendments in 2012. Under Section 69 of the Act, companies and their director, manager, secretary, or other company officers can be made liable for offences under the Act and punished accordingly unless they can prove their due diligence.[72]

In the digital age, content is free-flowing and the buttons of like, share and facility of the screenshot in all smartphones have changed the way content is circulated. The copyright act assigns liability on key persons of the company and allows exemption in case of due diligence; however, as the intent is difficult to prove and not always criminal, the misuse of the section is more likely than its fair use.

The businesses, though, enjoy protection under 52(1) (b) and (c) and Section 79 of the IT Act. However, courts' opinion is often different from the section's purpose. In a 2008 case, search engine Google was charged with Defamation for hosting a blog on its platform.[73] Google India had moved the High Court of Andhra Pradesh to dismiss the criminal charges against it because it enjoyed safe-harbour protection under Section 79 of the IT Act.[74]Google India failed to gain said protection as it did not take down the blog after information and now will face trial in the case.[75]

Intermediaries have been charged with copyright infringement in cases because by allowing viewership and sharing of pictures along with music, it has knowingly allowed for infringement and has become a party in the infringement.[76] The court adopted a similar point of view in the case of Kent RO Systems.[77]

There is a lack of clarity in the law concerning intermediaries, and it does not lay down the kind of content that is not permissible under the law of copyright. Intermediaries find themselves at a loss as to what action to take for any such content as they might be required to monitor, track, retain or delete any data as per the various laws in the country. As the intermediaries, to protect themselves from liability, have taken to censorship.[78]

Disproportionate action taken against digital businesses through Code of Criminal Procedure, 1973 (Cr.PC)

Section 91 of the Cr.PC allows the court to issue notices for presenting any document or file by means of summons. However, in a recent case, it has been observed that this provision is used by the law enforcement authorities to freeze accounts under the pretext of an investigation into a cheating case.[79]

Intermediary Liability Across Global Jurisdictions

In order to respond to new market players and businesses, governments need to develop clear, coherent rules to facilitate digital economic activities. It is fairly important for developing economies like India, which have not fully reaped the benefits of the digital evolution for economic growth.[80]

Making the employees personally criminally liable[81] may adversely affect the business sentiment of digital businesses, consequently leading to enterprises wanting to leave the

country, adversely affecting investments, employment, and welfare of the digital economy. Governments worldwide increasingly pressurise the intermediaries to block their users' undesirable content to suppress dissent, hate speech, privacy violations, and the like. These pressures often surface in making intermediaries legally responsible for the actions of their users.[82]

Marco Civil Da Internet of Brazil: A Civil Liability Framework for Intermediaries

Brazil is the only country with a specialised intermediary liability regime designed for Internet access providers and Internet application providers. The "Marco Civil" establishes exemptions to providers' liability in relation to third-party content, and access providers are always exempt from liability for user content and behaviour.[83]

The model chosen by Brazil in adopting its civil framework for the internet (Marco Civil da Internet) can be seen as an inspiration for the definition of principles underlying such global mechanisms. The model has two distinguishing provisions:

a. The multistakeholder nature of the process that led to the definition of the existing legal framework; and
b. the aspiration to give a "constitutional" dimension to such a framework, by recognising some fundamental rights and principles as founding pillars of internet regulation.[84]

The Marco Civil is also known as "constitution for the internet" because it revolves the whole regulatory framework around a number of guarantees for civil liberties, such as the privacy and freedom of expression of users.[85]

Another distinction in the Brazilian framework is that it distinguishes the intermediaries into two main categories (1) content producers who are publishers of content and (2) infrastructure providers who are not expected to detect or remove potentially illegal material.

Article 18 addresses the liability of Internet connection providers' liability and grants an exception to those services regarding intermediary liability. It states that "the Internet connection provider shall not be subject to civil liability for content generated by third parties".

The law introduced a liability exemption for *Internet connection providers* and the application of the safe harbour doctrine for other *Internet application providers*.

Article 19, which addresses Internet application providers (excluding connection providers) states that, "to ensure freedom of expression and to prevent censorship, an Internet application provider shall only be subject to civil liability for damages caused by virtue of content generated by third parties.

If, after a specific court order, an intermediary does not take action, according to the framework and technical limits of its services and within the time-frame ordered, to make the infringing content unavailable." For a literal interpretation of the law, neither the responsibility exemption to ICPs nor the safe harbour doctrine to ISPs would apply to criminal liability.[86]

Similar to Global Taxation of Tech Giants,[87] there is a need for a global regime of intermediary liability. Brazil's law based upon civil liability can provide the three base pillars for the development of intermediary liability regimes:

a. To identify the "constitutional ground" upon which an intermediary liability regime should be founded, supported by several principles safeguarding fundamental rights

while encouraging private enterprises.

b. To accept the necessity of having a multi-stakeholder drafting procedure to achieve consensus over basic intermediary liability principles. This procedure would expose the need for a differentiated intermediary liability regime, particularly, for copyright and "revenge porn", by defining specific exceptions to those principles.
c. To understand the unsuitability of a "one size fits all" approach and how differential treatment in intermediary liability legislation should be at the core of future intermediary liability discussions.[88]

Along with the civil liability framework of Brazil, there are several principle-based laws detailed below, which can be best practices to borrow for India's regulations.

Publisher Liability of Intermediaries

Australia was one of the first countries to pass online intermediary liability legislation in 1992. Decades later, in 2019, it passed an additional law. In early 2021, the Australian government had passed legislation to enact a news media bargaining code to " address bargaining power imbalances between Australian news media businesses and digital platforms, specifically Google and Facebook.[89]

In addition to the awareness shield under Article 3 of Japan's Provider Liability Limitation Act, Japan has also stated that when providers block content, they are not liable for "any loss incurred by" the user who posted the content, as long as providers meet one of two requirements. First, if they had "reasonable ground… to believe that the rights of others were infringed without due cause" by the content in question, they are not liable. Second, if they receive a takedown notice, they must ask the user who posted the content for consent to remove it—and if the user does not respond within seven days, they are also not liable.[90]

The United States of America, provides under the Digital Millennium Copyright Act (DMCA) that online services are not liable for their "good faith disabling of access to, or removal of, material or activity claimed to be infringing, … regardless of whether the material or activity is ultimately determined to be infringing."[91] Instead, any individual who files a takedown notice or counter-notice is liable if they "knowingly materially misrepresent" that either the content in question was infringing, or that it was not infringing and was mistakenly removed.[92]

Similar provisions find a place in the **South African** legislation. Similarly, under Chapter XI, Section 77 of South Africa's Electronic Communications and Transactions Act, websites are not liable for a wrongful takedown if they remove the content in response to a takedown notice. Rather, the individual who submitted the notice is liable for damages if they knowingly misrepresented the facts.[93]

Intermediary Liability for Third Party Actions

In Australia, similar to the Indian IT Act, Schedule 5, Clause 91 of Australia's Broadcasting Services Act 1992 states that websites and Internet service providers (ISPs) are not liable for third-party content under state or territory laws as long as they were "not aware of the nature" of the content.[94]

However, The Copyright Act 1968 creates a system of secondary liability, expressly providing that infringement occurs if a person authorises an infringing act. part V div 2AA of the Copyright Act protects 'service providers' from copyright infringement in certain circumstances. The Australian High Court confirmed that where the publisher of a message is a 'mere conduit', the publisher is not liable.[95]

The Copyright Act 1968 is the only legislation to expressly attribute liability to an e-commerce platform where that platform has authorised an infringing act. The Federal Court held that Redbubble (an e-commerce platform)

had communicated the copyrighted work (primary infringement); and secondary infringement would be made out.[96] Thus implying that platform operators will only be liable where they have been found to authorise copyright infringement (that is, the platform operator has enabled others to infringe copyright).[97]

The United States of America offers a unique and interesting case, from both a legal and policy perspective, to study the governance landscape for online intermediaries. The Communications Decency Act's Section 230 prevents online intermediaries from being treated as the publisher of content from users of the intermediaries.[98] Section 230 covers defamation, invasion of privacy, tortious interference, civil liability for criminal law violations, and general negligence claims based on third-party content. Section 230 also contains a few major exceptions; notably, its liability shield does not apply to federal criminal law, state or federal sex trafficking law, or intellectual property law instead of India's list of exemptions on public order, national security, etc.

South Africa's Electronic Communications and Transactions Act, enacted two years after the EU's E-Commerce Directive, contains sections on mere conduit in a similar language. South Africa's law does not include awareness or "actual knowledge" provisions. However, it does state that online services that meet the requirements for mere conduit, caching, or hosting must still comply with any court order to remove unlawful content.[99]

Liability Shield provisions for Intermediary

The United States has a separate law, the DMCA, that governs online copyright law. In the United States, the DMCA states that an online service is not liable for third-party content that violates copyright law if "upon obtaining such knowledge or awareness, it acts expeditiously to remove, or disable access to, the material." Once platforms become aware of potentially harmful or illegal content, it is often easier for platforms to remove it immediately to avoid liability rather than determine whether the content breaks any laws.

Japan is one of the most technologically advanced countries. It has also provided broad awareness protection to intermediaries, where intermediaries are not liable unless they have actual knowledge. Article 3 of Japan's Provider Liability Limitation Act, enacted in 2001, contains a liability shield that does not apply if a provider is aware that third-party content causes "the infringement of the rights of others," or if "there is a reasonable ground to find" that they know this.[100]

Instances of Businesses Exiting Markets Due to Increasing Regulations

In Hong Kong, with recent changes to data protection law[101] against the prevalent doxing where people put other person's personal information online so others can harass them[102], the law has prescribed criminal investigation and prosecution of the employees of tech companies for doxing offences by their users.[103] According to an industry coalition of tech companies based in Hong Kong, Facebook, Google and Twitter have reportedly already hinted at leaving the country if the proposed legislation prescribing criminal liability is implemented.[104]

According to these companies, refraining from investments and service offerings would only avoid sanctions on them under the proposed law.

In China, in October 2021, LinkedIn exited the Chinese market citing "challenging operating environment" as the cause when the Chinese government increased its scrutiny.[105] It is worth noting that the Chinese Personal Information Protection Law was passed by the Chinese Standing Committee of the National People's Congress on August 20, 2021 and was effective from November 01, 2021.[106] The Article

71 of the law contains criminalising provisions that may have been a cause for LinkedIn's exit.

In India, META reportedly wanted to call it quits as it fears the data privacy law could force it to modify or cease existing business practices under the DP Bill, 2021 as it fears that it could face fines, orders restricting or blocking its services, or other government-imposed remedies as a result of content hosted on its platform.[107] Though the threat was later recalled, it still implies the sentiments of big digital businesses towards the regulatory landscape.

Large digital platforms, services, and marketplaces provide small businesses with affordable, scalable, and secure business solutions. They have opened up new markets and allowed small businesses to compete globally and in unimaginable ways a few decades ago.[108]

As per a recent report,[109] criminality was never a part of punitive action against businesses in ancient India, and only financial penalties were. If any of the intermediaries decide to leave India due to over-regulations and criminalisation; no matter how far-fetched the notion is, the first impact will be on thousands of small businesses that use these platforms. Small businesses are the backbone of the Indian economy and represent India's spirit of start-up India and innovation.

Way Forward

Criminalisation provisions are neither novel nor novice in the business regulations. A recently released report[110] highlighted 26,134 different ways of going to jail for doing business in India. This number is alarming because such provisions deter new businesses from entering the market in India and impact their operations and day-to-day functioning, thus making it difficult for the businesses to operate. As businesses aid the economy to grow, such criminalising provisions are harmful to the country's economy, which the government is trying to improve.

The criminal jurisprudence in the country finds it appropriate to place criminal liability on a business; by extension on its employees in higher-ranking positions. However, a company is a legal person and not a natural person cannot be ignored. A legal person devoid of intent; can only act on intent of its employees; and in cases of non-compoundable offences; should be liable to be punished.

Below are some recommendations that can be used to make the framework of criminality for digital businesses more conducive and less imposing.

Adoption of Civil Liability Framework

India will benefit from adopting a framework similar to Brazil's where instead of segregating social media companies through the number of users; a division of businesses or platforms can happen based on roles, responsibility and capacity.

Each case should be evaluated on a subjective basis on merit, and before such evaluation, no imprisonment of an employee or ascertaining of liability should be done. The instant FIR and imprisonment nudge the judicial system towards a 'guilty until proven innocent approach' as opposed to much accepted in India 'innocent until proven guilty approach'.

Liability Shield

Intermediaries must be shielded by law from liability for third Party Content as any rules governing intermediary liability must be provided by laws, which must be precise, clear, and accessible. Under the IT Act framework, intermediaries should be immune from liability for third-party content in circumstances where they have not been involved in modifying that content. Similarly, a provision can be introduced under the Copyright Act to limit the liability of intermediaries not modifying the content to a notice-to-notice requirement. Suppose the IT

Act and the Copyright Act incorporate similar notice-and-notice regimes. In that case, the amended Copyright Act may specifically provide that the responsibilities for intermediaries shall be governed by the provisions of Section 79 of the IT Act.

Laws with Imprisoning clauses must Satisfy the Test of Necessity and Proportionality

The sections with minor economic offences under the PSSA should be moved to a show-cause notice requirement. Sections 26(1) and (4) should be reassessed on the proportionality of punishment and then the sections should be decriminalised as per the Finance Ministry's proposal.

Section 85 under IT Act allows for directors to be held liable for any infringement of the Act along with Rule 7 of Intermediary Rules, 2021, with similar intent. The vague and ambiguous language of these sections must be amended and transparency and accountability be built into laws.

Rule 4 of Intermediary Rules 2021 specifies the specific qualification of the CCO, which borders on infringing in the internal business matters of a corporation. This section must be tested on the ground of proportionality and over-prescriptive regulations must be avoided. The test of Proportionality prescribed under the *Puttaswamy Judgement*[111] should be the cornerstone for any law that takes away any right.

Repealing laws without adequate safeguards to protect the interest of citizens and Intermediaries

Since a country's regulations are framed for the betterment of its citizens and economy, any law which does not provide adequate safeguard must be abolished in favour of a better law. As observed by the Supreme Court, Section 69 A of the IT Act alongside the Blocking rules has practically unused safeguards and should not remain in force for preventing misuse.

The Criminal sanctions on intermediaries for non-compliance with government orders under the Blocking Rules would need to be repealed as being disproportionate and creating a chilling effect on the freedom of expression.[112] The upcoming Data Protection Bill, 2021 places disproportionate responsibilities on digital businesses instead of the government, before being brought in force Section 85, similar to IT Act, would need to be assessed on vagueness, proportionality and necessity.

It is important that the regulator proceeds with the intent of promoting Ease of Doing Digital Business in India while framing new legislations and assessing the existing ones.

Endnotes

1 'India's trillion-dollar digital opportunity' *available at* India's Trillion Dollar Digital Opportunity
2 Baird, Forrest E. and Koffman, Walter. ìPhilosophic Classics Volume IV. Nineteenth-Century Philosophy.î 2nd Edition. Prentice Hall Press. Upper Saddle River, New Jersey. 2000.
3 Tiwari, Piyush, 'DOCTRINE OF PROPORTIONALITY: AN ANALYSIS OF SUPREME COURT CASES', October 13, 2018, Racolb Legal, *available at* Doctrine of Proportionality: An analysis of Supreme Court cases | RACOLB LEGAL
4 Tauro Lionel, 'India: The Limited Liability Of Intermediaries For Third Party Content', 7 April 2021, Mondaq, *available at* The Limited Liability Of Intermediaries For Third Party Content - Media, Telecoms, IT, Entertainment - India
5 Aiyar, Shankkar, 'Archaic laws criminalise entrepreneurs', 13 February 2022, The New Indian Express, *available at* Archaic laws criminalise entrepreneurs.
6 Press Trust of India, 'Govt steps improving India's ease of doing business rank: Commerce ministry', 24 October 2019, Business Standard, *available at* Govt steps improving India's ease of doing business rank: Commerce ministry | Business Standard News
7 Krishnan, KP and Ravi Venkatesan, 'Making business easy: A template to ramp-up state capacity', 17 June 2021, Economic Times, *available at* MSMEs: Making business easy: A template to ramp-up state capacity - The Economic Times
8 Tungekar, Bushra MS, 'Decriminalization of compoundable company law offences', 29 January 2021, *available at* Decriminalization of compoundable company law offences - iPleaders
9 Govt clears amendments to LLP Act; to decriminalise 12 offences under law, 28 July 2021, Business Standard, *available at* Govt decriminalises Companies Act to promote greater ease of doing business | Business Standard News
10 Murshedd, Suhana Islam, Mitra, Shounak, Ease Of Doing Business Gains Momentum With The Latest Amendments To The LLP Act, 21 February 2022, Mondaq, *available at* Ease Of Doing Business Gains Momentum With The Latest Amendments To The LLP Act - Corporate/Commercial Law - India
11 Government of India Ministry of Finance Department of Financial Services *** 8th June, 2020 Statement of Reason: Decriminalisati
12 Tandon, Suneera, 'Retailers urge DIPP to decriminalize LM Act', 16 December 2022, Mint, *available at* Retailers urge DIPP to decriminalize LM Act
13 Section 79, IT ACt, 2000 *available at* Section 79 in The Information Technology Act, 2000
14 Singh, Shubham, 'What does Section 79 of IT Act mean for social media intermediaries?', May 28, 2021, Zee News, *available at* Explained: What does Section 79 of IT Act mean for social media intermediaries? | Technology News | Zee News
15 Pandey, Jyoti, 'The Supreme Court Judgement in Shreya Singhal and What It Does for Intermediary Liability in India?', 11 April 2015, Centre for Internet and Society, available at The Supreme Court Judgement in Shreya Singhal and What It Does for Intermediary Liability in India? — The Centre for Internet and Society
16 Agarwal, Shubhra and Agarwal, Anusha, 'Section 67 of IT Act 2000: Scope, Misuse and the Striking Inadequacy', 2 June 2020, Criminal Law Blog National Law University, Jodhpur, *available at* Section 67 of IT Act 2000: Scope, Misuse and the Striking Inadequacy
17 Avnish Bajaj vs State (N.C.T.) Of Delhi on 21 December, 2004 (2005) 3 CompLJ 364 Del, 116 (2005) DLT 427, *available at* Avnish Bajaj vs State on 29 May, 2008
18 Ekta Kapoor v. State Of M.P, on 11.11.2020, Madhya Pradesh High Court, *available at* Ekta Kapoor vs State Of MP on 11 November, 2020
19 'Complaint against Ekta Kapoor's Alt Balaji dismissed due to lack of evidence by cyber police', 3 June 2020, PinkVilla, *available at* Complaint against Ekta Kapoor's Alt Balaji dismissed due to lack of evidence by cyber police | PINKVILLA
20 'Madhya Pradesh HC refuses to quash case against Ekta Kapoor', 12 November 2020, The Hindu, *available at* Madhya Pradesh HC refuses to quash case against Ekta Kapoor - The Hindu
21 'SC Grants Interim Protection From Arrest To Ekta Kapoor In FIR In 'XXX Season 2' Controversy', 17 December 2020, News ABP Live, *available at* SC Grants Interim Protection From Arrest To Ekta Kapoor In FIR In 'XXX Season 2' Controversy
22 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, *available at* Procedure and Safeguards for Interception, Monitoring and Decryption
23 Rule 21 under the 2009 Rules.
24 Apar Gupta v. Ministry Of Home Affairs, Central Information Commission, *available at* Apar Gupta vs Ministry Of Home Affairs on 31 January, 2022
25 'Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State', 14 January 2019, The Wire, *available at* Why Five Petitions Are Challenging the Constitutional Validity of India's Surveillance State
26 Jalan, Pranay, 'Guest Post: Resolving the Good Samaritan Paradox: An Enabler for Proactive Content Moderation?', 1 October 2021, Indian Constitutional Law and Philosophy, *available at* intermediary liability – Indian Constitutional Law and Philosophy
27 X v. Union of India and Ors., 20 April 2021, Delhi High Court *available* at X vs Union Of India And Ors. on 20 April, 2021
28 ABC v. DEF and Ors., 24 September 2020, Delhi High Court, *available at* https://indiankanoon.org/doc/77617707/
29 'Information Technology (Intermediary guidelines and Digital media ethics Code) Rules, 2020' *available at* https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf
30 Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016. available at Information Technology (Prese...r Facilities) Rules, 2016

[31] Regidi, Asheeta, 'The Indian Government proposes new data retention rules:will privacy be compromised?', 14 October 2016, First Post, *available at* The Indian government proposes new data retention rules: Will privacy be compromised?- Technology News, Firstpost

[32] Bharadwaj Deeksha, 'Centre may tweak IT Act, bring in new penalties', 16 September 2021, Hindustan Times, *available at* Centre may tweak IT Act, bring in new penalties | Latest News India - Hindustan Times

[33] Shreya Singhal v. Union of India, (2013) 12 S.C.C. 73.

[34] 'Supreme Court Upholds Freedom of Speech on the Internet', Lexology, *available at* Supreme Court Upholds Freedom of Speech on the Internet - Lexology

[35] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, *available at,* Information Technology (Blocking Rules), 2009

[36] S, Aishwarya, 'Information Technology (Blocking Rules), 2009 and Section 69a of the IT Act, 2000', 22 November 2021, Ipleaders, *available at* Information Technology (Blocking Rules), 2009 and Section 69a of the IT Act, 2000 - iPleaders.

[37] Deol, Taran, 'All about Section 69A of IT Act under which Twitter had withheld several posts & accounts', 2 February, 2021, The Print, *available at* All about Section 69A of IT Act under which Twitter had withheld several posts & accounts

[38] Sabu Mathew George v. Union of India and Ors., *available at* Sabu Mathew George vs Union Of India And Ors. on 13 December, 2017

[39] Joshi, Divij, 'Indian Intermediary Liability Regime Compliance with the Manila Principles on Intermediary Liability', Centre for Internet and Society, *available at* Indian Intermediary Liability Regime

[40] 'India's Surveillance State', 2014, SLFC, *available at* https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf

[41] Regidi, Asheeta, 'The Indian Government proposes new data retention rules:will privacy be compromised?', 14 October 2016, First Post, *available at* The Indian government proposes new data retention rules: Will privacy be compromised?- Technology News, Firstpost

[42] Rule 2(w) under the Intermediary Rules, 2021.

[43] 'Govt sets 50 lakh users threshold to define 'significant social media intermediary' under IT rules', February 27, 2021, Economic Times, *available at* Govt sets 50 lakh users threshold to define 'significant social media intermediary' under IT rules - The Economic Times

[44] How the intermediaries' rules are anti-democratic and unconstitutional.

[45] To ensure compliance with the Information Technology Act, 2000 and Intermediary Rules.

[46] To ensure 24x7 coordination with law enforcement agencies to ensure compliance with orders made in accordance with law.

[47] To enforce redressal grievance mechanism as per Rule 3(2) of the Intermediary Rules.

[48] Under Rule 4(a) it is stated that The Chief Compliance officer can be made liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Act and rules made thereunder. This is subject to an opportunity of being heard.

[49] 'Platforms with over 50 lakh users to be 'significant social media intermediaries', February 28, 2021, The Indian Express, *available at* Platforms with over 50 lakh users to be 'significant social media intermediaries' | Technology News,The Indian Express

[50] Saraswathy, M and Swathi Moorthy, 'Fat salary but bigger risks: Is this a tech job that nobody wants?', 6 July, 2021, Money Control, *available at* Fat salary but bigger risks: Is this a tech job that nobody wants?

[51] Section 2(51) of Companies Act, 2013 gives the definition of Key Managerial Person.

[52] Saraswathy, M and Swathi Moorthy, 'Fat salary but bigger risks: Is this a tech job that nobody wants?', 6 July, 2021, Money Control, *available at* Fat salary but bigger risks: Is this a tech job that nobody wants?

[53] 'Twitter transfers India head Manish Maheshwari to US, assigns new role of senior director', 13 August 2021, The Print, *available at* Twitter transfers India head Manish Maheshwari to US, assigns new role of senior director

[54] Incidents of lynching and mob violence have been reported from videos and messages circulated on the WhatsApp platform in India. For reference, *Viral WhatsApp Messages Are Triggering Mob Killings In India*, July 18, 2018, Lauren Frayer, *available at* Viral WhatsApp Messages Are Triggering Mob Killings In India : NPR

[55] Singh, Vikram Jeet; Mara, Prashant; India: Liable vs. Accountable: How Criminal Use Of Online Platforms And Social Media Poses Challenges To Intermediary Protection In India; May 2020; Mondaq; *available at* Liable vs. Accountable: How Criminal Use Of Online Platforms And Social Media Poses Challenges To Intermediary Protection In India - Media, Telecoms, IT, Entertainment - India

[56] October 2021 https://www.meity.gov.in/writereaddata/files/FAQ_Intermediary_Rules_2021.pdf

[57] Bharadwaj, Deeksha, 'Centre may tweak IT Act, bring in new penalties', September 16, 2021, Hindustan Times, *available at* Centre may tweak IT Act, bring in new penalties | Latest News India - Hindustan Times

[58] MouthShut.com v. Union of India, WRIT PETITION (CIVIL) NO. OF 2013, *available at* MouthShut.com v/s Union of India - Supreme Court - Freedom of Expression

[59] Authorisation for operations provided under Section 7, PSSA, 2007 *available at* Payment and Settlement Systems Act, 2007

[60] Section 4, PSSA, 2007 *available at* Payment and Settlement Systems Act, 2007

[61] 'Offences Which Do Not Provide a Minimum Sentence of 7 Years Imprisonment Are Not Heinous: SC', January 10, 2020, The Wire, *available at* Offences Which Do Not Provide a Minimum Sentence of 7 Years Imprisonment Are Not Heinous: SC

[62] Section 299, IPC, 1860.

63 Whoever commits culpable homicide not amounting to murder, shall be punished with imprisonment for life, or imprisonment for either description of a term which may extend to 10 years.
64 Obhan, Ashima and Dua, Akanksha, 'Decriminalization of Minor Economic Offences: A Step towards 'Sabka Saath, Sabka Vikas and Sabka Vishwas'', 18 August 2020, Lexology, *available at* Decriminalization of Minor Economic Offences: A Step towards 'Sabka Saath, Sabka Vikas and Sabka Vishwas' - Lexology
65 'Cheque bouncing will no longer be criminal offence?', Babushahi Bureau, 12 June 2020, *available at* https://www.babushahi.com/full-news.php?id=103124&headline=Cheque-bouncing-will-no-longer-be-criminal-offence
66 Recommendation 6, JPC Report on PDP Bill, 2019.
67 Shreya Singhal v. Union of India, AIR 2015 SC 1523.
68 Section 66A empowered police to make arrests over what policemen, in terms of their subjective discretion, could construe as "offensive" or "menacing" or for the purposes of causing annoyance, inconvenience, etc.
69 Avinash Bajaj v. State, 2008 (150) DLT 769.
70 My Space Inc. v. Super Cassettes Industries Ltd.,236 (2017) DLT 478.
71 Tauro L (2021) The Limited Liability Of Intermediaries For Third Party Content. Mondaq, *available at* The Limited Liability Of Intermediaries For Third Party Content - Media, Telecoms, IT, Entertainment - India
72 Section 69, Copyright Act, 1957, *available at* the copyright act, 1957 (14 of 1957)
73 Google v. Visakha Industries, [Criminal Petition No. 7207 of 2009], *available at* Google India Private Ltd vs M/S. Visakha Industries on 10 December, 2019
74 Intermediary Liability 2.0: A Shifting Paradigm, SFLC, Licensed under CC BY-SA-NC 4.0, *available at* INTERMEDIARY LIABILITY 2.0: A SHIFTING PARADIGM
75 Bharadwaj, Prachi, ' Google India fails to gain protection under Section 79 of the IT Act, 2000; To face trial in a 2008 defamation case', 11 December 2019, SCC Online, *available at* Google India fails to gain protection under Section 79 of the IT Act, 2000; To face trial in a 2008 defamation case | SCC Blog
76 My Space Inc. vs Super Cassettes Industries Ltd, 23 December, 2016, Delhi high court, *available at* My Space Inc. vs Super Cassettes Industries Ltd. on 23 December, 2016.
77 Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors, 18 January, 2017, Delhi High Court, *available at* Kent Ro Systems Ltd & Anr vs Amit Kotak & Ors on 18 January, 2017.
78 'Liability of Online Intermediaries under the Copyright Regime', 10 February, 2021, Kashish IPR, *available at* Liability of Online Intermediaries under the Copyright Regime.
79 Joshi, Neha, 'Alibaba.com moves Bombay High Court against account freezing in cheating case', 10 March 2022, Bar and Bench, *available at* Alibaba.com moves Bombay High Court against account freezing in cheating case
80 Chen, Rong, 'Policy and Regulatory Issues with Digital Businesses', July 2019, World Bank Policy Research Working Paper 8948, *available at* Policy and Regulatory Issues with Digital Businesses
81 Rule 4(1) (a) of Intermediary rules 2021.
82 INTERMEDIARY LIABILITY, Center for Internet and Society, *available at* Intermediary Liability | Center for Internet and Society
83 Canabarro, Diego Rafael and Real, Paula, Corte, 'Mapping Intermediary Liability in Latin America', 21 August 2020, Internet Society, *available at* Mapping Intermediary Liability in Latin America - Internet Society
84 Zingales, Nicolo, 'The Brazilian approach to internet intermediary liability: blueprint for a global regime?', 28 December 2015, Internet Policy Review, DOI: 10.14763/2015.4.395, *available at* The Brazilian approach to internet intermediary liability: blueprint for a global regime? | Internet Policy Review
85 Brazil's Superior Court of Justice, Fourth Panel, Google Brazil, Special Appeal no. 1306157/SP, 24 March 2014.
86 'Marco Civil da Internet - "Brazilian Civil Rights Framework for the Internet', 23 April 2014, WILMAP Stanford, *available at* Marco Civil da Internet - "Brazilian Civil Rights Framework for the Internet" | wilmap
87 Bartz, Diane, 'Big tech supports global tax, but wants digital services levies axed', 9 June 2021, Reuters, *available at* Big tech supports global tax, but wants digital services levies axed | Reuters
88 Zingales, Nicolo, 'The Brazilian approach to internet intermediary liability: blueprint for a global regime?', 28 December 2015, Internet Policy Review, DOI: 10.14763/2015.4.395, *available at* The Brazilian approach to internet intermediary liability: blueprint for a global regime? | Internet Policy Review
89 Barata, John and Pappalardo, Kylie, 'Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021', 3 March 2021, Stanford, *available at* Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act 2021 | wilmap
90 Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Japan, 2001), Article 3, Clause 2.
91 17 U.S. Code § 512 - Limitations on liability relating to material online, *available at* 17 US Code § 512 - Limitations on liability relating to material online
92 *Ibid.*
93 Electronic Communications and Transactions Act, 2002 (Republic of South Africa), Chapter XI, Section 77.
94 Broadcasting Services Act 1992 (Commonwealth of Australia), Schedule 5, Clause 91.
95 Google Inc v. ACCC (2013) 249 CLR 435, *available at* https://jade.io/j/?a=outline&id=289620
96 In Hells Angels Motorcycle Corporation (Australia) Pty Ltd v. Redbubble Ltd (2019) 140 IPR 172, *available at* https://jade.io/j/?a=outline&id=638087

97 Kamath, Raunak, 'Internet Committee Publishes Report on Intermediary Liability in Asia-Pacific Region', 10 November 2021, INTA, *available at* Internet Committee Publishes Report on Intermediary Liability in Asia-Pacific Region - International Trademark Association

98 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material, *available at* 47 US Code § 230 - Protection for private blocking and screening of offensive material

99 Electronic Communications and Transactions Act, Chapter XI, Section 73-75.

100 Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Japan, 2001), Article 3, Clause 1.

101 Personal Data (Privacy) Ordinance, Hong Kong *available at* 《個人資料(私隱)條例》 Personal Data (Privacy) Ordinance

102 Purnell, Newley, 'Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws', July 5, 2021, The Wall Street Journal, *available at* Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws - WSJ

103 MacAllister, Julia M. , 'The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information' , 85 Fordham L. Rev. 2451 (2017). *Available at:* https://ir.lawnet.fordham.edu/flr/vol85/iss5/44

104 Purnell, Newley, 'Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws', July 5, 2021, The Wall Street Journal, *available at* Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws - WSJ

105 'After LinkedIn's exit from China, will more companies follow suit?', October 16, 2021, Business Standard, *available at* After LinkedIn's exit from China, will more companies follow suit? | Business Standard News

106 Personal Information Protection Law of the Mainland, *available at* Personal Information Protection Law of the Mainland

107 'Meta ready to throw in towel', 4 March 2022, India Business Law Journal, *available at* Meta ready to throw in towel | India Business Law Journal

108 Ward, Jake, 'Digital big tech drives small business success', November 19, 2019, the Hill, *available at* https://thehill.com/opinion/technology/471005-digital-big-tech-drives-small-business-success

109 'Jailed for Doing Business', February 10, 2022, ORF, *available at* Jailed For Doing Business | ORF.

110 'Jailed for Doing Business', February 10, 2022, ORF, *available at* Jailed For Doing Business | ORF.

111 Justice K.S.Puttaswamy(Retd) v. Union Of India, 26 September, 2018, *available at* Justice KSPuttaswamy(Retd) vs Union Of India on 26 September, 2018

112 Joshi, Divij, 'Indian Intermediary Liability Regime Compliance with the Manila Principles on Intermediary Liability', Centre for Internet and Society, *available at* Indian Intermediary Liability Regime

This Discussion Paper was authored by Neelanjana Sharma, Senior Research Associate, CUTS International. The author gratefully acknowledges the contribution of Amol Kulkarni, Director (Research) and Prince Gupta, Senior Research Associate, CUTS International to this paper.

March 2022