Primer for an Information Technology Framework Law / Working Paper

V | D H | Centre for Legal Policy

About the Authors

This working paper is an in-progress draft, prepared as an independent non-commissioned piece of work by the Vidhi Centre for Legal Policy, an independent think-tank doing legal research to help make better laws.

Aniruddh Nigam and Kadambari Agarwal are Research Fellows at the Vidhi Centre for Legal Policy. Trishi Jindal and Jai Vipra are Project Fellows at the Vidhi Centre for Legal Policy.

The authors would like to thank Dr. Arghya Sengupta and Mr. Supratim Chakraborty for their comments on earlier drafts of the working paper.

Summary

Objectives of the working paper:

- ***Reforming the Information Technology Act, 2000***
  This working paper briefly summarises the approach proposed to be adopted in the formulation of a blueprint for a new legislation to replace the Information Technology Act, 2000 for India. The Information Technology Act, 2000 **('IT Act')** is the primary law governing the internet in India. The developments of the previous decades have presented several fresh challenges in the realm of internet governance, which the IT Act fails to holistically address. Thus, there is a need to re-visit the Act to adapt it to the modern state of the digital environment.

- ***Formulating an agenda for reform***
  This working paper will be followed by a series of in-depth concept papers which set out the theoretical framing and regulatory design of a new legislation to govern the digital environment in India. As the first step in this exercise, it is necessary to consolidate various issues related to technology policy in an inclusive approach. This working paper proposes an approach that may be followed in the development of such a legislation.

Part I: Need for holistic reform

This part of the working paper discusses the current state of the regulation of information technology in India by the IT Act, and some criticisms of the same. It is suggested that these criticisms point to a fundamental recasting of the role that a law like the IT Act should play, given the broad nature of the field of information technology, the rapid pace of technological growth and the reliance on delegated legislation to make substantive rules.

Part II: A framework legislation for information technology

This part of the working paper suggests that the IT Act should be recast in the role of a framework law. It discusses the concept of framework legislation, and identifies that in the field of information technology, a framework law can work as a 'digital constitution' – by setting out basic digital rights, placing limits on State and private action and establishing institutions for coordination, collective action and enforcement.

Part III: Designing a framework legislation

This part of the working paper looks at how a framework legislation which operates as a digital constitution may be designed. It identifies three lines of inquiry which form the analytical exercise that must be undertaken to design a framework law for information technology.

Appendix I: Consolidation of issues under the IT Act

The appendix of the working paper contains a detailed mapping of various provisions of the IT Act, grouped into issues and sub-issues which form the crux of substantive regulation under the Act. This enables a meaningful discussion for reform of these individual issues, by aggregating the provisions which relate to each issue.

I. Need for holistic reform

A. The existing state of the law

- The regulation of information technology in India is primarily undertaken through the IT Act. The IT Act contains provisions which address a wide-ranging variety of issues – from the recognition of electronic documents and signatures, to data protection and privacy and the regulation of content online. This wide scope of the IT Act makes it a seminal legislation setting the contours of the exercise of the rights and obligations in the information technology sphere in India. It contains both substantive provisions and offences, as well as an extensive body of delegated legislation to clarify the governance or crucial issues under the Act.

- However, the IT Act is not sufficiently robust at dealing with many of these issues.[1] The dated nature of several provisions of the Act also raises concerns about its efficacy. For example, the reductive definition of 'intermediary' under the Act contains within its sweep a wide variety of entities ranging from social media platforms to internet service providers and cyber cafes.[2] This has led to various calls for the recognition of specific kinds of intermediaries within the ambit of the Act.[3] Similar criticisms are often levelled at many other parts of the IT Act – the criminal provisions are broadly and vaguely worded and do not address specific harms[4], most procedural safeguards under the Act are outdated, and the provisions are not sufficiently harmonised with other related laws.[5]

- Further, for many aspects which are currently governed by the IT Act, the need for specialised legislation to address these aspects has also emerged since its last substantive amendment in 2008. A prominent example is the personal data protection framework, which is currently covered to a limited extent under Section 43A of the IT Act, and the IT (Reasonable Security Practices and Procedures) Rules, 2011.[6] However, the recognition of the right to privacy as a fundamental right, and the consequent need for a detailed framework for the protection of personal data has led to development of the draft Personal Data Protection Bill, 2019, which is intended to set out a detailed legislative framework and obligations related to the protection of personal data.[7]

- These dual trends – the dated nature of some of the provisions of the Act, and the movement towards considering specialised legislation for matters governed by the Act – point to a more fundamental recasting of the role of the IT Act. Embedding substantive rules within the law runs the risk of such rules being outmoded by the development of technology and the change of the socio-economic context within

[1] Sudipto Dey, 'Why India's IT Act needs an overhaul', BUSINESS STANDARD, available at < https://www.business-standard.com/article/opinion/why-india-s-it-act-needs-an-overhaul-116100900734_1.html> Accessed 24th August 2020; N S Nappinai, 'Cyber Security and Challenges: Why India need to Change IT Act', CYBER PEACE FOUNDATION (2017), available at <https://www.cyberpeace.org/CyberPeace/Repository/20180412-IT-Act-Need-for-Laws-to-Spruce-Up-02.02.2018-1.pdf> Accessed 25th August, 2020.

[2] *See* Section 2(1)(w), Information Technology Act, 2000.

[3] Varun Sen Bahl, Faiza Rahman and Rishab Bailey, 'Internet intermediaries and online harms: Regulatory responses in India', Data Governance Network Working Paper 06 (2020) ("Discussing the challenges with a one-size-fits-all approach to regulation of intermediaries")

[4] Amlan Mohanty, 'New crimes under the Information Technology (Amendment) Act', 7 INDIAN JOURNAL OF LAW AND TECHNOLOGY, 103, 120 (2011) ("Discussing the definitional ambiguities of the criminal provisions in the Information Technology Act")

[5] N S Nappinai, 'Cyber Security and Challenges: Why India need to Change IT Act', CYBER PEACE FOUNDATION (2017), available at <https://www.cyberpeace.org/CyberPeace/Repository/20180412-IT-Act-Need-for-Laws-to-Spruce-Up-02.02.2018-1.pdf> Accessed 25th August, 2020.

[6] *See* Section 43A, Information Technology Act, 2000; Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

[7] Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna on a Free and Fair Digital Economy, Ministry of Electronics and Information Technology.

which those rules were drafted.[8] For example, the social significance of online platforms has undergone a massive change over the past few years. This role, however, is not reflected in the provisions relating to their responsibility, which were drafted nearly a decade ago.[9] The slow pace of parliamentary review further makes the embedding of substantive rules in the law an unwieldy method of regulating rapidly evolving information technology.

- This simultaneously affects the degree of detail which can be provided in the law, since these details are likely to be outmoded in the near-future, or technological workarounds to these details are likely to be discovered.[10] This has led to a situation where granular regulatory detail is usually found in Rules and Regulations under the Act. However, the processes through which these Rules are ordinarily drafted are often not deliberative or accountable. There is a need to correct this in any regulatory framework for information technology.

B. Criticisms of the legal framework

1. Lack of a conceptual framework

- The IT Act was initially drafted for the limited purpose of recognising electronic documents and transactions. Over time, mostly ad-hoc amendments to the Act have expanded its scope to several other issues. However, **the IT Act lacks a coherent conceptual framework** through which it can be understood.[11]

- The common thread which runs through the many issues governed by the IT Act is a proximate connection to the idea of technology, where technology refers to the infrastructure of, and entities on, the internet. Additionally, the Act, in some cases, applies to other electronic systems which are used for processing information, and other peripheral issues which can arguably be related to the idea of 'information technology'. While this may offer a common theme, it arguably does not completely satisfy the requirement of coherence. Coherence requires that the rules under a legislation be part of "*a system of rules that fit together in a consistent, logically elaborated pattern*",[12] or that they be "*connected by some sort of logical relationship to each other*".[13] The ad-hoc expansion of the scope of the IT Act is in part responsible for this lack of coherence.

- It is important that the scope of regulation of the IT Act be clearly delineated and have a coherent conceptual basis to it. This requires an understanding of the harms, functions, and effects that the IT Act is intended to regulate. These harms, functions and effects must be connected to each other through a logical relationship. This can enable the expansion of the law to other issues where this logical relationship is satisfied. This conceptual thread can take the form of a system of harms, or can take the form of a set of rights related to which rules are made. For example, the White Paper on Online Harms, released in the United Kingdom, contains a systematic review of the kinds of harms that are intended to

[8] Bert-Jap Koops, 'Should ICT Regulation be technology-neutral?' in STARTING POINTS FOR ICT REGULATION: DECONSTRUCTING PREVALENT POLICY ONE LINERS (Bert-Jap Koops *et al* ed., TMC Asser Press), 1, 2 (2006) ("Discussing the phenomenon of governmental attempts to regulate being out-moded by the time they are finally enacted with respect to technology-specific regulation")

[9] Varun Sen Bahl, Faiza Rahman and Rishab Bailey, 'Internet intermediaries and online harms: Regulatory responses in India', Data Governance Network Working Paper 06 (2020) ("Discussing the evolved social significance of intermediaries"); Information Technology (Intermediary Guidelines) Rules, 2011.

[10] Lawrence Lessig, Code v2.0, 118 (2006) ("Discussing the use of circumvention technologies to weaken rules reinforcing control")

[11] *See* Roger Brownsword, 'Law and Technology: Two Modes of Disruption, Three Legal Mindsets and the Big Picture of Regulatory Responsibilities', 14(2), INDIAN JOURNAL OF LAW AND TECHNOLOGY, 1, 15, 2018 ("Discussing the value of 'regulatory coherentism' to establishing regulatory legitimacy, where 'coherentism' is understood as the emphasis on a set of rules being connected by some sort of logical relationship to each other"); *See also* Edward L Rubin, 'From Coherence to Effectiveness' in RETHINKING LEGAL SCHOLARSHIP, 310 (R. Van Gestel *et al* eds., Cambridge University Press) 2017.

[12] Edward L Rubin, 'From Coherence to Effectiveness' in RETHINKING LEGAL SCHOLARSHIP, 310, 328 (R. Van Gestel *et al* eds., Cambridge University Press) 2017.

[13] Edward L Rubin, 'From Coherence to Effectiveness' in RETHINKING LEGAL SCHOLARSHIP, 310, 313 (R. Van Gestel *et al* eds., Cambridge University Press) 2017.

be tackled by the development of a regulatory framework.[14] A similar exercise is necessary in order to find a conceptual thread that anchors any legislation governing the internet.

2. Reliance on delegated legislation

- The field of information technology is so broad that it is impossible to account for all aspects of this field in a single legislation. This has led to the IT Act adopting the use of delegated legislation for making substantive rules about most subject-matters. There are two concerns with this. *First*, rules must not expand or travel beyond the scope of the Act.[15] However, with ever-expansive rules being proposed, this is likely to happen. *Second*, there is a **need to provide for deliberative and accountable processes for rule making** under legislation which relates to fields as broad as information technology, and will inevitably come to rely on delegated legislation.

- For example, the IT Act contains merely the broad 'safe harbour' for intermediaries on the internet, while their granular responsibilities are set out in the Information Technology (Intermediary Guidelines) Rules, 2011.[16] Similarly, the IT Act merely authorises that security practices and procedures for 'protected systems' may be enacted, but the substantive practices and procedures are found in the Information Technology (Security Practices and Procedures for Protected Systems) Rules, 2018.[17] The same is true for other key issues, such as the procedure through which content may be blocked[18] or through which law enforcement may intercept information.[19] While a reliance on delegated legislation is inevitable, the processes which lead to the enactment of this delegated legislation must be designed in a manner which preserves public agency in the law-making process. It is necessary to establish institutions which achieve this purpose in the operation of any law which governs a field as broad as information technology and is inevitably going to rely on delegated legislation.

- Given the rapid pace of technological development and the variety of aspects under consideration, it may not be possible to embed all substantive rules related to the regulation of various technologies within legislation. In this regard, it is necessary that any legislation "*outlines the main substantive principles that are at stake*",[20] and provides a deliberative procedure through which specific regulation may be enacted under this law.

3. Need for future-proof regulation

- The law will inevitably struggle to keep pace with technology. While legislation may be drafted with a certain state of technology in mind, technological progress will create the need for the law to play catch-up.[21] This either takes the form of reactive and ad-hoc law-making, or ill-conceived regulation.[22] There is a need to future-proof any legislation on technology which can govern the digital environment regardless of the specific technological context. To this end, it is important that as a starting point, any

[14] Online Harms White Paper, Presented to the Parliament by the Secretary of State for Digital, Culture, Media and Sport and the Secretary of State for the Home Department by Command of Her Majesty, April 2019 [United Kingdom], available at < https://www.gov.uk/government/consultations/online-harms-white-paper> Accessed 23rd August 2020

[15] Dr. Mahachandra Prasad Singh v. Chairman, Bihar Legislative Council, 2004 8 SCC 747 at ¶ 13.

[16] *See* Section 79, Information Technology Act, 2000; Information Technology (Intermediary Guidelines) Rules, 2011.

[17] Information Technology (Security Practices and Procedures for Protected Systems) Rules, 2018

[18] Information Technology (Procedure and safeguards for blocking for access of information by public) Rules, 2009

[19] Information Technology (Procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009.

[20] Bert-Jap Koops, 'Should ICT Regulation be technology-neutral?' in STARTING POINTS FOR ICT REGULATION: DECONSTRUCTING PREVALENT POLICY ONE LINERS (Bert-Jap Koops *et al* ed., TMC Asser Press), 1, 25 (2006) ("Discussing the need to differentiate at levels of regulation and the need for legislation to indicate fundamental rights, values and the rationale that underlies regulation")

[21] Bert-Jap Koops, 'Should ICT Regulation be technology-neutral?' in STARTING POINTS FOR ICT REGULATION: DECONSTRUCTING PREVALENT POLICY ONE LINERS (Bert-Jap Koops *et al* ed., TMC Asser Press), 1, 2 (2006) ("Discussing the phenomenon of governmental attempts to regulate being out-moded by the time they are finally enacted with respect to technology-specific regulation")

[22] Akriti Gaur and Arghya Sengupta, 'To keep up with Tiktok & Bitcoin, India needs innovation in lawmaking too', THE PRINT, available at < https://theprint.in/opinion/to-keep-up-with-tiktok-bitcoin-india-needs-innovation-in-lawmaking-too/249778/> Accessed 23rd August, 2020

regulation **identifies technology-neutral standards and rights** which can govern the digital environment regardless of the specific technological context.[23] This is currently absent.

- The idea of "technology-neutral" standards here implies that the same regulatory principles should apply regardless of the technology used.[24] This requires that laws are not drafted in technological silos,[25] and directly contributes to the sustainability of the law.[26] Technology-neutrality assumes even greater importance considering the gamut of new technologies that are in development or are likely to be widely used in the near future. For example, technologies like wearables, facial recognition technologies, drones and devices connected to the Internet-of-Things are all likely to witness large scale adoption in the near future. While granular rules which govern the specifics of these technologies are necessary, at the same time, some broad principles must be developed which run across these technologies. For example, any offence related to the intrusion of privacy, or unauthorised access into a device, should apply regardless of the specific technology used. Similarly, the right to not be denied access to a public facility due to a lack of technological access should be guaranteed, regardless of the technology deployed in that facility.

- Additionally, there are many issues related to internet governance which have assumed prominence over the previous few decades, and a new legislation must be capable of dealing with these challenges. For example, the growth of the digital economy in many sectors has been led by significant online platforms – a phenomenon which has led to monopolisation of various industries[27] and a concentration of power and digital intelligence in privately owned and governed companies.[28] This has serious implications for the economic development of a domestic digital ecosystem, as well as for the civil and political rights of Indian citizens. In addition to fostering transparency and accountability for such entities in the short term, there is a need to ensure that India possesses the capability to engage with the global digital economy on its own terms.[29] In this pursuit, it is equally important to locate the individual at the centre of any regulatory framework, and to develop legal rights and entitlements which safeguard the interests of the individual in the digital environment.

[23] Bert-Jap Koops, 'Should ICT Regulation be technology-neutral?' in STARTING POINTS FOR ICT REGULATION: DECONSTRUCTING PREVALENT POLICY ONE LINERS (Bert-Jap Koops *et al* ed., TMC Asser Press), 1, 1 (2006) ("Discussing technology-neutrality as a starting point for developing ICT Regulation")

[24] Winston Maxwell and Marc Bourreau, 'Technology neutrality in Internet, telecoms and data protection regulation', COMPUTER AND TELECOMMUNICATIONS LAW REVIEW (2014) ("Discussing the multiple meanings of the phrase technology-neutral")

[25] Winston Maxwell and Marc Bourreau, 'Technology neutrality in Internet, telecoms and data protection regulation', COMPUTER AND TELECOMMUNICATIONS LAW REVIEW (2014) ("Discussing the multiple meanings of the phrase technology-neutral")

[26] Bert-Jap Koops, 'Should ICT Regulation be technology-neutral?' in STARTING POINTS FOR ICT REGULATION: DECONSTRUCTING PREVALENT POLICY ONE LINERS (Bert-Jap Koops *et al* ed., TMC Asser Press), 1, 1 (2006) ("Discussing technology-neutrality as a starting point for developing ICT Regulation")

[27] There is significant literature discussing the 'platform economy' – where platforms are understood as multi-sided markets. Multi-sided markets produce both direct and indirect network effects, in addition to reducing coordination costs, thereby occupying a central role in structuring exchange in the market. Economic research on the operation of multi-sided markets suggests that the production of network effects tends towards a winner-take-all scenario in the market, leading to the creation of monopolies in various industries. *See* Jean Charles-Rochet and Jean Tirole, 'Two sided markets: A progress report', 37(3), THE RAND JOURNAL OF ECONOMICS, 645 (2006); David S Evans and Richard Schmalensee, 'The antitrust analysis of multi-sided platform businesses', NBER Working Paper No w18783 (2013); Andrei Hagiu and Julian Wright, 'Multi-sided Platforms', INTERNATIONAL JOURNAL OF INDUSTRIAL ORGANISATION, 43 (2015).

[28] Parminder Jeet Singh, 'Data and Digital Intelligence Commons (Making a case for their community ownership), DATA GOVERNANCE NETWORK WORKING PAPER 02 (2019) ("Discussing the concentration of digital intelligence in private companies")

[29] Parminder Jeet Singh, 'Developing countries in the emerging global digital order – A critical geopolitical challenge to which the Global South must respond', 2017, available at < https://itforchange.net/developing-countries-emerging-global-digital-order> Accessed 23rd August, 2020 ("Discussing the need for developing countries to not get locked in patterns of digital dependency")

II. A framework legislation for information technology

- In pursuance of the above-stated objectives, we propose that a new legislation be enacted to replace the IT Act. This legislation, which we tentatively refer to as **The Information Technology and Digital Rights Act (ITDR Act)** is proposed to be developed as a 'framework law'. This part of the working paper explores the concept of a framework law and develops this concept specifically in the context of information technology. It is proposed that the ITDR Act be formulated within the theoretical framing of 'digital constitutionalism', and a system of basic rights and entitlements form the coherent conceptual basis of this Act. Further, the practical imperative to ensure continuity of existing regulation is also considered in the framing of the ITDR Act as a 'digital constitution'.

1. What is a framework legislation?

- The phrase "framework law" is often used to refer to laws which structure rulemaking in a particular policy area.[30] These laws can contain some fundamental principles which should govern future policy related to this area. Additionally, they establish procedures and institutions which govern the enactment of legislation or delegated legislation related to this area.

- While the term "framework law" does not find entrenchment in legal doctrine, there are several examples of laws which have been considered by scholars to be "framework laws".[31] The feature of framework laws which distinguish them from ordinary laws providing for delegated legislation is the fact that they also establish rules for how the delegated legislation is to be enacted, and provide some fundamental principles to which such delegated legislation should conform. These laws serve many purposes – in addition to the symbolism provided by these laws, they set out "*neutral rules of procedure*"[32] and enable these rules to be applied to situations that are not immediately foreseeable.

- The regulation of broad fields like information technology requires any legislation to account for situations that are immediately foreseeable, as well as for situations that are likely to arise later. This leads to lawmakers working with a "*partial veil of ignorance*",[33] given that the concrete issues and desired outcomes may not be specifically identifiable at the time of making the law. This requires the legislation to set out "*neutral rules*" – that is, procedures which effectively shape deliberation to counteract self-interest and bias in future rule-making.[34] Since the specific outcomes that are desired in every issue cannot be known, the focus of a framework law is to develop procedures which allow for such issues to be regulated in a fair and unbiased manner.[35]

[30] Elizabeth Garrett, 'The purposes of framework legislation', 14 JOURNAL OF CONTEMPORARY LEGAL ISSUES, 717 (2004) ("Discussing the concept of framework legislations")

[31] Elizabeth Garrett, 'The purposes of framework legislation', 14 JOURNAL OF CONTEMPORARY LEGAL ISSUES, 717 (2004) ("Discussing the lack of systematic study of framework laws")

[32] Elizabeth Garrett, 'The purposes of framework legislation', 14 JOURNAL OF CONTEMPORARY LEGAL ISSUES, 717 (2004) ("Discussing the purposes fulfilled by framework laws")

[33] Elizabeth Garrett, 'The purposes of framework legislation', 14 JOURNAL OF CONTEMPORARY LEGAL ISSUES, 717 (2004) ("Discussing the concept of a partial veil of ignorance in the formulation of framework laws where lawmakers are not aware of which outcomes are desirable to them and which procedures which help them or hurt them in the future")

[34] Adrian Vermeule, 'Veil of ignorance rules in constitutional law', 111 YALE LAW JOURNAL, 399 (2001) ("Discussing the formulation of fair procedures when operating in a partial veil of ignorance and the factors that lead to the development of neutral rules")

[35] Elizabeth Garrett, 'The purposes of framework legislation', 14 JOURNAL OF CONTEMPORARY LEGAL ISSUES, 717 (2004) ("Discussing the proposition that for a framework law to succeed as neutral rules of decision, it must eliminate avenues for evasion once concrete issues emerge")

- The ITDR Act can achieve the objectives mentioned in Part I of this paper by operating as a framework legislation. **Framework legislations are instruments that are like constitutions for a subset of issues.**[36] The ITDR Act will be the constitution of the digital economy.

2. Enacting a digital constitution

- In the context of the internet, the idea of 'framework legislations' ties into the theory of 'digital constitutionalism'.[37] While there are multiple meanings that are given to this phrase, it most commonly implies initiatives which seek to fulfil the functions of constitutions in the digital sphere. Classically, the idea of constitutionalism refers to the mechanisms which limit the boundaries of a state's power over its citizens,[38] by providing citizens with fundamental rights and entitlements and establishing institutions for coordination, collective action and protecting those rights.[39] The idea of 'digital constitutionalism', when studied in the context of virtual communities, has also been understood to imply limitations on the power of private actors,[40] given that "*in today's political economy of the Internet, states and private corporations alike can either limit or contribute to the realisation of perceived digital rights.*"[41] This formulation appears to be the synthesised academic view on the concept of 'digital constitutionalism' as well.[42]

- We adopt this theoretical framing to study how individual rights in the digital environment may be institutionalised in an effective and comprehensive manner. The ITDR Act, operating as a digital constitution, would perform the following functions:

    - **Articulate overarching rights for Indian citizens** in the digital environment and define the limits of state and private action in relation to these rights.

    - **Establish institutions and processes** for future rule making, enforcement and coordination between authorities for securing these rights.

3. Continuity of regulation

- At the same time, we must recognise that replacing the IT Act cannot create a vacuum of regulation. Therefore, a new legislation would have to **continue substantively regulating many aspects which are covered by the erstwhile IT Act** and add certain substantive facets of regulation that have emerged today (such as platform governance, treatment of non-personal data, etc.). The identification of these aspects would ensure that any new framework governing the internet does not lead to a withdrawal of the State from the public sphere, but instead, appropriately identifies how the State must interact with the participants of the digital economy.

[36] Elizabeth Garrett, 'The purposes of framework legislation', 14 JOURNAL OF CONTEMPORARY LEGAL ISSUES, 717 (2004)

[37] Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism: Mapping attempts to craft an Internet Bill of Rights', 80(4), INTERNATIONAL COMMUNICATIONS GAZETTE (2018) ("Discussing initiatives which belong to the conversation of digital constitutionalism")

[38] Carl J Freidrich, 'Constitutional Government and Democracy: Theory and Practice in Europe and America', 35 (4th ed., 1968) ("Discussing constitutionalism as an effective regularized restraint on governments"); *See also* Jeremy Waldron, 'Constitutionalism: A Skeptical View' in CONTEMPORARY DEBATES IN PHILOSOPHY, 267 (2009).

[39] Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism: Mapping attempts to craft an Internet Bill of Rights', 80(4), INTERNATIONAL COMMUNICATIONS GAZETTE (2018) ("Discussing a definition of digital constitutionalism")

[40] Nicolas Suzor, 'The role of the rule of law in virtual communities', 25(4) BERKELEY TECHNOLOGY LAW JOURNAL, 1817 (2010) ("Discussing the role of private commercial actors in ordering interactions in virtual communities and digital constitutionalism as the articulation of limitations on their power")

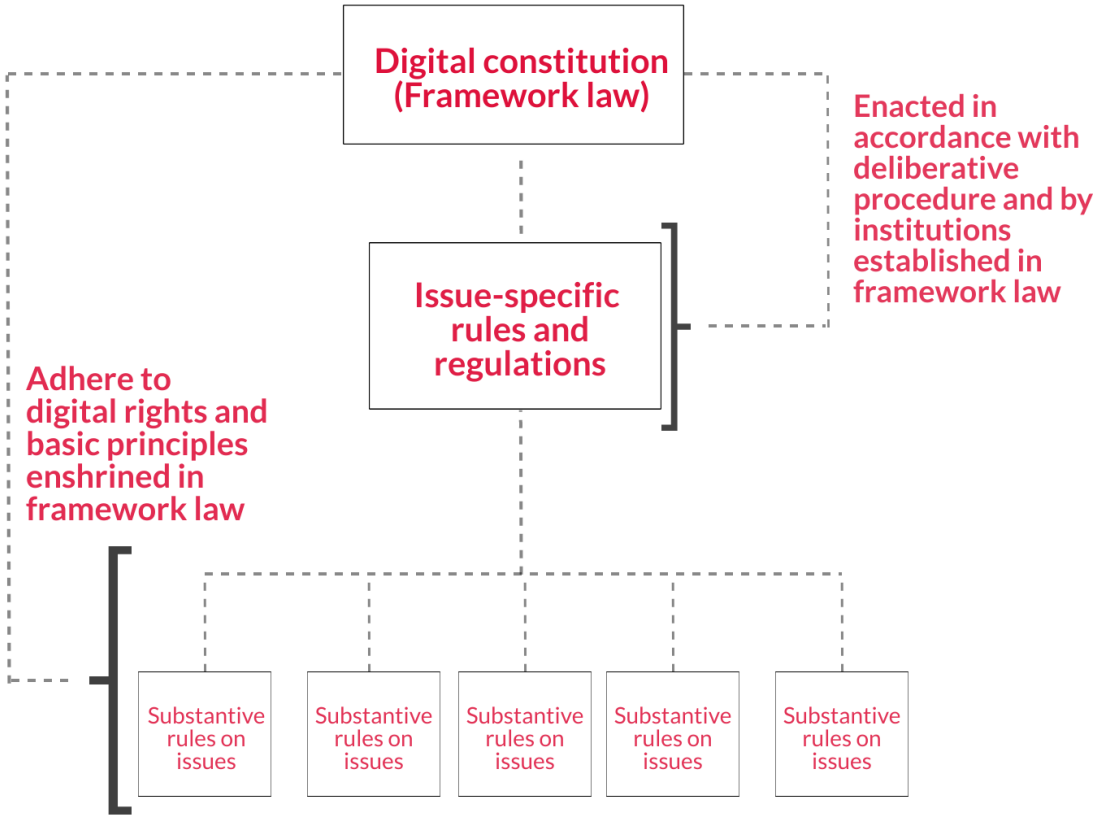
[41] Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism: Mapping attempts to craft an Internet Bill of Rights', 80(4), INTERNATIONAL COMMUNICATIONS GAZETTE (2018) ("Discussing the extent of the phrase digital constitutionalism")

[42] Edoardo Celeste, 'Digital Constitutionalism: a new systematic theorisation' INTERNATIONAL REVIEW OF LAW, COMPUTERS AND TECHNOLOGY (2019) ("Reviewing the many uses of the phrase digital constitutionalism and presenting a synthesized version of this idea")

III. Designing a framework legislation

- In this part of the working paper, we identify how the ITDR Act may be designed to operate as a framework law for the purposes of governing information technology. The first step of this process is identifying the way a framework law operates, which enables us to identify the specific inquiries that must be conducted to develop a blueprint for the ITDR Act.

- The following illustration depicts the way a framework legislation operating as a digital constitution can govern substantive subject-matters and illustrates the functions that it fulfils:



- In line with this scheme, to develop a blueprint for the ITDR Act in alignment with the theory of 'digital constitutionalism', the following three-pronged approach is proposed, which encapsulates the necessary inquiries to in the formulation of a framework law: (a) the identification of digital rights and basic principles; (b) the identification of substantive issues which merit regulation; and (c) the identification of rulemaking procedures and institutions to be established under the Act:

I. Identification of a charter of rights for the digital environment

- The first step in the analytical exercise is to **discover a formulation of digital rights which protects the interests of the individual**. This includes both adaptations of established civil rights (freedom of speech, right to private communications), as well as novel rights which are arguably specific to the digital environment (net neutrality rights, the right to internet access, the right against technological exclusion from public facilities).[43] An example of this would be the Brazilian Civil Rights Framework for the Internet - which adapts various civil and political rights to the digital context.[44] There have also been several civil society initiatives in this regard that provide valuable guidance towards the formulation of such rights.[45]

- This exercise would also define the boundaries of state and private infringement of these rights, thereby authorising 'reasonable restrictions' on certain grounds. Constitutional restrictions on state authorities already exist, though the precise nature of those restrictions is often undefined due to a lack of jurisprudence specifically relating to the digital environment. Additionally, this exercise would be novel in **restricting private infringement of these rights**. The identification of these limitations on State and private power is necessary for civil and political rights as well as economic rights. The Report of the Committee of Experts on Non-Personal Data initiates this conversation in the context of economic rights over non-personal data.[46] and limitations on state and private action can be derived from the principles of this report, as well as the critical evaluation of these proposed limitations.

II. Identification of substantive issues from the IT Act which would continue being regulated

- As discussed above, principally, legal reform should not signify a withdrawal of the State from the public sphere. Additionally, there is a strong practical imperative for the continued regulation of issues that are already regulated. Broadly, this would include some of the following issues:

• *Recognition of electronic documents and signatures*

The recognition and regulation of electronic documents and signatures under the IT Act is largely based on the Model Law on Electronic Commerce, 1996 ("MLEC") and Model Law on Electronic Signatures 2001 ("MLES") published by the United Nations Commission on International Trade Law ("UNCITRAL"). In 2017, UNCITRAL published the Model Law on Electronic Transferable Records ("MLETR"), which enables the legal use of electronic transferable documents that are functionally equivalent to paper-based transferable documents. So far, Indian legislation has not moved towards harmonizing the law on electronic signatures and documents with the MLETR. For example, Section 3A(2) of the IT Act prescribes reliability standards in respect of electronic signatures which are used to authenticate electronic records, which are heavily borrowed from the MLES. However, the MLETR has introduced other standards for ensuring reliability in respect of authentication of an electronic transferable document, such as applicable industry standards, security of the hardware and the software, etc. Novel

[43] Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism: Mapping attempts to craft an Internet Bill of Rights', 80(4), INTERNATIONAL COMMUNICATIONS GAZETTE (2018) ("Discussing the substantive content of initiatives characterized as digital constitutions")

[44] Marco Civil Law of the Internet in Brazil, Law No. 12.965, 2014 [Brazil]

[45] Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism: Mapping attempts to craft an Internet Bill of Rights', 80(4), INTERNATIONAL COMMUNICATIONS GAZETTE (2018) ("Discussing multiple attempts to craft an Internet Bill of Rights")

[46] Report by the Committee of Experts on Non-Personal Data Governance Framework, MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, available at < https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf> Accessed 23rd August, 2020

reliability standards are only one example; the provisions of the MLETR must be studied and adapted to the needs of the Indian IT space.

Further, the IT Act does not apply to certain documents/transactions (for example, negotiable instruments except cheques), as listed under Schedule I. Given the increased need for conducting business and transactions digitally, there is a need to revisit why these documents have been excluded from the purview of the IT Act and make the necessary amendments to the IT Act. Additionally, novel issues in relation to electronic signatures and the public key infrastructure must be considered in a reform of these provisions. For example, digital signatures have been almost prohibitively expensive for use by ordinary individuals, and measures which can make such technologies more accessible may be considered.[47]

- ***Regulation of electronic service delivery***

The Information Technology (Electronic Service Delivery) Rules, 2011 ("ESD Rules") currently only prescribe minimum standards in respect of delivery of electronic services.[48] Given their limited scope, the ESD Rules have failed to address many issues relevant to electronic service delivery. For example, though the ESD Rules enable the delivery of such services, they neither ensure equal public accessibility to these services nor mandate establishing an alternative (and non-electronic) means to avail those services. This is likely to have unfavourable implications for many Indians due to unequal access to internet connectivity.[49] Another example is that the ESD Rules have left the prescription of security standards in relation to electronic service delivery transactions, to the discretion of the government, under Rule 3(3).[50] In the absence of stringent security standards, the safety of personal data used in electronic transactions can be compromised, and also lead to additional difficulties in setting up a viable system of electronic service delivery. Given that the law on electronic service delivery has lacunae which are not addressed by the ESD Rules, the need for comprehensive statutory prescriptions related to electronic service delivery remains unfulfilled.

Further, the ESD Rules are an example over-expansive delegated legislation. The ESD Rules were made under Section 87(2)(ca) read with Section 6A of the IT Act, which allows specifically for the authorisation and regulation of service providers in respect of electronic service delivery.[51] However, Rule 3(1) authorizes Central/State Governments to provide electronic services on their own, subjecting them to the same standards as an authorised service provider.[52] The articulation of standards for service delivery by authorised service providers, and by governments themselves, must pay specific attention to the obligations of the State and create effective regulatory standards for authorised service providers. Notwithstanding that such authorization goes beyond the scope of the IT Act and is an instance of expansive delegated legislation, it is necessary to provide substantive legal protections to individuals in respect of service delivery by Governments as well as by authorised service providers with nuanced attention paid to the division of responsibilities in this exercise. This exercise must also provide for fundamental entitlements and rights that must be guaranteed in any service delivery. These must be provided in the framework legislation governing information technology.

[47] Jayakumar Thangavel, 'Digital Signature: Comparative study of its usage in developed and developing countries', Thesis for the degree of Master in Information Systems Sciences submitted to Uppsala University (2014) ("Discussing regulatory initiatives related to digital signatures aimed at increasing their adoption")

[48] Information Technology (Electronic Service Delivery) Rules, 2011

[49] Internet and Mobile Association of India and Nielson, 'Digital in India 2019: Round 2 Report', accessed 31st August 2020.

[50] Rule 3(3), Information Technology (Electronic Service Delivery) Rules, 2011.

[51] Section 6A, Information Technology Act, 2000.

[52] Rule 3(1), Information Technology (Electronic Service Delivery) Rules, 2011.

- ## *Confidentiality and security of computer resources*

  Penalties and offences for ensuring confidentiality of information and security of computer resources are necessary for ensuring public trust in the electronic communication infrastructure.[53] The IT Act, thus provides civil[54] and criminal[55] penalties for damaging, gaining unauthorised access to, or destroying a 'computer resource'. It further provides civil and criminal penalties for unauthorised access to, damage to, theft of source code.

  However, this framework as it stands requires a concerted review. Specifically, the language employed in these sections is, in many cases, over-broad and does not provide clear guidance on the scope of activities that are permitted under the Act.[56] The framework does not create a distinction between accidental and intentional acts where civil penalties are prescribed.[57] Similarly, for white hat hackers and security researchers, necessary liability protections are absent for sharing necessary information with the cyber security authorities.[58] Additionally, the current framework for securing personal data and ensuring its privacy and confidentiality is expected to be revised under the Personal Data Protection Bill, 2019. To this end, the new Act will need to be rationalised with surviving provisions, especially relating to the security of personal data.

- ## *Cybercrime, offences, and penalties*

  There needs to be a fresh review of the actions that are criminalised under IT laws. The IT Act as it stands criminalises identity theft and fraud, non-consensual access and capturing of private information, child pornography, sexually explicit content and cyber terrorism. It has been criticised for ambiguous wording and broad definitions that leave too much room for interpretation and unduly criminalise conduct.[59] For example, Section 66F of the IT Act, while defining cyber terrorism, includes actions that threaten not just the sovereignty and integrity of India, the security of the State and friendly relations with foreign States, but also includes conduct that threatens "public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise".[60] The inclusion of conduct such as 'defamatory conduct' under cyber terrorism, which does not bear a clear nexus with concept of 'terrorism' has been criticised as posing a threat to civil liberties.[61] Additionally, while the erstwhile Section 66A of the IT Act was struck down by the Supreme Court, on grounds of it being void-for-vagueness,[62] there continues to be a

[53] Claudia Sarrocco, 'Elements and principles of the Information Society', International Telecommunications Union, available at <https://www.itu.int/osg/spu/wsis-themes/Access/BackgroundPaper/IS%20Principles.pdf> Accessed 23rd August, 2020

[54] Section 43, Information Technology Act, 2000.

[55] Section 66, Information Technology Act, 2000.

[56] Karan Saini, Pranesh Prakash, et al, 'Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India', Centre for Internet and Society, available at <https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf/view> Accessed 1st September, 2020.

[57] Karan Saini, Pranesh Prakash, et al, 'Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India', Centre for Internet and Society, available at <https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf/view> Accessed 1st September, 2020.

[58] Karan Saini, Pranesh Prakash, et al, 'Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India', Centre for Internet and Society, available at <https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf/view> Accessed 1st September, 2020.

[59] A scoping of the criminal law in the UK and its application to various harms witnessed online reflected the need to revise laws to address specific harms to ensure freedom of speech protections. See 'Law Commission of the United Kingdom, Abusive and Offensive Online Communications: A Scoping Report', Law Com No. 381 (2018), available at <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/10/6_5039_LC_Online_Comms_Report_FINAL_291018_WEB.pdf> Accessed 23rd August, 2020.

[60] Section 66F, Information Technology Act, 2000.

[61] Malavika Jayaram, 'Civil Liberties and the amended Information Technology Act, 2000', The Centre for Internet & Society, available at <https://cis-india.org/internet-governance/blog/information-technology-act> Accessed 1st September, 2020.

[62] Shreya Singhal v. Union of India, 2015 5 SCC 1.

need to criminalise some of the kinds of conduct that was otherwise covered by that section.[63] For example, vitriolic gender-based or caste-based abuse has increased manifold online, and in the absence of narrowly tailored provisions which attach to such behaviour, the IT Act often leaves victims of abuse without sufficient redress.

Criminal provisions in the IT Act also overlap with parts of the Indian Penal Code (IPC). For example, Sections 43 and 66 of the IT Act deal with some conduct that is already criminalised by many provisions of the IPC.[64] In some cases, however, there may be dimensions to this behaviour that cannot be fully comprehended under the remit of the IPC and may instead be more appropriately placed in the ITDR Act, given that it is the special law governing online harms. A detailed and systemic examination of particular kinds of 'cybercrime' which merit criminal liability under this law is necessary to create an effective framework for criminal liability which simultaneously respects the civil liberties of individuals.

- ***Content regulation***

The IT Act, as it stands, provides the government with powers to block certain kinds of content under Section 69A of the Act. This power is provided in respect to content which relates to the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States, public order or for preventing the incitement of a cognisable offence in relation to these grounds.[65] This is a limited sub-set of the grounds which are permissible restrictions on the freedom of speech and expression under Article 19(2) of the Constitution. Most of these grounds relate to issues which would generally be referred to as "*national security*" issues, in addition to the ground of "*public order*", which may refer to a slightly wider set of behaviour. However, governmental processes to regulate some other kinds of content, such as blocking non-consensual transmission of sexual imagery or requiring mandatory fact-checking of some kinds of misinformation, are lacking under this legislation. The desirability of these powers, and other similar sophisticated powers, may be evaluated considering the evolving nature of digital communications.

Additionally, offending content is often hosted on platforms which are structured as intermediaries. These intermediaries, by virtue of the Supreme Court's interpretation of intermediary liability in *Shreya Singhal*, are not required to take down such content unless they receive a court order or a government order under Section 69A of the Act.[66] It has often been noted that the requirement to procure a court order may impose undue costs and delays on victims of online abuse,[67] and the need for imposing proactive content regulation in respect of narrowly tailored categories of content may be necessary. This is especially true given the existing capabilities of many significant intermediaries, the influence they wield over public communications and the unique position they occupy to proactively monitor their platforms.[68] This should not imply a limitation of free speech online, and the creation of appropriate procedures – such as a notice-and-notice system of taking down content, providing for an appeal mechanism for proactive content regulation and other mechanisms which can institute the concept of due process in online content regulation – may help achieve a balance between the rights of a complainant, internet users and intermediaries.[69]

[63] *See*, for example, the Harmful Digital Communications Act, 2015 [New Zealand]

[64] Vinod Joseph and Diya Ray, 'Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence', National Seminar on Cyber Crime and Cyber Warfare at Symbiosis Law School, Hyderabad (2020), available at <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence> Accessed 1st September, 2020.

[65] Section 69A, Information Technology Act, 2000.

[66] Shreya Singhal v. Union of India, 2015 5 SCC 1.

[67] Amrita Vasudevan, 'Taking down cyber violence: Supreme Court's emerging stance on online censorship and intermediary liability', 2 ECONOMIC AND POLITICAL WEEKLY (2019) ("Discussing the failure and shortcomings of the existing legal regime in addressing cyber violence")

[68] Giancarlo F Frosio, 'Why keep a dog and bark yourself? From intermediary liability to responsibility', 26(1) INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY (2018) ("Discussing the evolution of laws related to intermediary liability over the previous few years")

[69] Amrita Vasudevan, 'Taking down cyber violence: Supreme Court's emerging stance on online censorship and intermediary liability', 2 ECONOMIC AND POLITICAL WEEKLY (2019) ("Discussing the failure and shortcomings of the existing legal regime in addressing cyber violence")

- ***Regulation of intermediaries***

The IT Act contains a one-size-fits-all definition of 'intermediaries', which as explained in the first part of this paper, includes a wide variety of entities – ranging from internet service providers to social media platforms and cyber cafes.[70] Online intermediaries, however, have grown in complexity and influence over the previous few decades. There is a dire need to recognise different kinds of intermediaries and enact a sophisticated framework for their regulation, which appropriately distinguishes between different 'layers' of the Internet.[71] The concept of the 'safe harbour' – which refers to the immunity from liability provided to an intermediary for third-party content – must be refined keeping in mind the differentiated nature and influence of various intermediaries.

Over the last few years, many jurisdictions have witnessed the imposition of greater responsibility on some kinds of intermediaries.[72] For example, the European Commission has explicitly recommended the imposition of duties of proactively monitoring the content on their platforms on certain kinds of social media intermediaries.[73] Any imposition of responsibility on intermediaries must be formulated keeping in mind the design of such intermediaries – to ensure that the imposition of responsibility is fair, just and attuned to the capabilities of the intermediary.[74]

Additionally, the regulation of intermediaries in India has largely been through the lens of either judicial intervention,[75] or through the "due diligence" requirements that an intermediary must fulfil to avail their immunity from liability for user-generated content.[76] Neither of these mechanisms creates statutorily enforceable duties on online intermediaries. Given the significant nature and variety of harms that can emerge from activities on these platforms and their influence over public communications, it may be appropriate to impose enforceable duties on such intermediaries, which are punishable by law, in line with their design aspects.

- ***Law enforcement assistance***

Section 69 of the IT Act provides the government with powers to intercept, monitor or decrypt any information[77] after following the procedure laid out in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.[78] These rules provide very wide powers to be exercised upon issuance of orders by the Secretary of Home Affairs in the Central Government, and the Secretary of the Home Department in State Governments.[79] A 2019 office order of the Ministry of Home Affairs allows for these orders to be issued by these functionaries to ten law enforcement agencies designated under this provision, who carry out the necessary actions under this order.[80] This scheme creates an expansive framework for law enforcement assistance and

[70] Varun Sen Bahl, Faiza Rahman and Rishab Bailey, 'Internet intermediaries and online harms: Regulatory responses in India', Data Governance Network Working Paper 06 (2020)

[71] Lawrence B Solum, 'The layers principle', 79(3) NOTRE DAME LAW REVIEW, 815 (2004) ("Discussing the use of 'layers' as a method for conceptualising regulation of the Internet")

[72] Giancarlo F Frosio, 'Why keep a dog and bark yourself? From intermediary liability to responsibility', 26(1) INTERNATIONAL JOURNAL OF LAW AND INFORMATION TECHNOLOGY (2018) ("Discussing the evolution of laws related to intermediary liability over the previous few years")

[73] 'Tackling illegal communication online: Towards an enhanced responsibility of online platforms', COM(2017) 555 Final, European Commission.

[74] Oliver Sylvain, 'Intermediary Design Duties', 50 CONNECTICUT LAW REVIEW, 203 (2018) ("Discussing the concept of intermediary design duties which are attuned to the design aspects of intermediaries")

[75] Amrita Vasudevan, 'Taking down cyber violence: Supreme Court's emerging stance on online censorship and intermediary liability', 2 ECONOMIC AND POLITICAL WEEKLY (2019); Varun Sen Bahl, Faiza Rahman and Rishab Bailey, 'Internet intermediaries and online harms: Regulatory responses in India', Data Governance Network Working Paper 06 (2020)

[76] *See* Section 79(3)(b), Information Technology Act, 2000; Information Technology (Intermediary Guidelines) Rules, 2011

[77] Section 69, Information Technology Act, 2000.

[78] *See* Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

[79] Rule 2(d), Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

[80] Ministry of Home Affairs, S.O. 6227(E), Order [No. 14/07/2011-T]

surveillance and has often been criticised for lacking sufficient procedural safeguards.[81] Meaningful surveillance reform requires that these powers be reviewed and formulated in a narrow manner, focusing on the values of transparency and accountability in the issue of orders for interception, monitoring and decryption of information.

Additionally, law enforcement in India has been noted to rely on pre-digital era procedural powers, such as Section 91 of the Code of Criminal Procedure, 1973 to compel the production of information.[82] This creates a decentralised system of seeking access to information in the digital domain.[83] To standardise this process, create necessary procedural safeguards and improve transparency in the scheme of law enforcement assistance, it is necessary to develop standard operating procedures, and possibly, a single-window mechanism, which dictates how law enforcement may seek access to information in a computer resource.

- ***Cybersecurity authorities and related powers***

Cybersecurity authorities remain vital for coordinating emergency response and information and expertise sharing with their global counterparts for cyber security threats, breaches, vulnerabilities, and securing critical information infrastructure.[84] To this end, the Computer Emergency Response Team (CERT-In) is set up under the IT Act to serve as the nodal agency to undertake computer emergency responses and coordinate with sectoral and global CERTs on security matters.[85] The National Critical Information Infrastructure Protection Centre (NCIIPC) is designated as the nodal agency for critical information infrastructure protection.[86] Its mandate extends to designating sectors as CII and sub-sectors as protected systems, and prescribing sectoral guidelines, among other functions such as capacity building, information sharing, etc. The effectiveness of these authorities has however remained limited.

The IT Act framework currently does not provide sufficient incentives to drive active information sharing, which is crucial to early detection and response to cyber security incidents, by researchers, white hat hackers, and private entities alike.[87] Specifically, the NCIIPC's structuring under an intelligence agency does not allow for transparency and sufficient coordination with industry participants within sectors designated as CIIs.[88] Similarly, the security related provisions within the IT Act are broadly worded and run the risk of creating disincentives to security research.[89] Limited capacity within these organisations and the lack of harmonisation among different authorities and their roles has further created challenges to ensuring public interface and encouraging their participation in

[81] Aniruddh Nigam, 'India's expanding surveillance scheme violates right to privacy', OxHRH Blog, 5 January 2019.

[82] Tarun Krishnakumar, 'Law enforcement access to data in India: Considering the past, present and future of Section 91 of the Code of Criminal Procedure, 1973' 15 INDIAN JOURNAL OF LAW AND TECHNOLOGY, 67 (2019). ("Discussing the law and practices related to law enforcement access to data in India")

[83] Tarun Krishnakumar, 'Law enforcement access to data in India: Considering the past, present and future of Section 91 of the Code of Criminal Procedure, 1973' 15 INDIAN JOURNAL OF LAW AND TECHNOLOGY, 67 (2019). ("Discussing the law and practices related to law enforcement access to data in India")

[84] Claudia Sarrocco, 'Elements and principles of the Information Society', INTERNATIONAL TELECOMMUNICATIONS UNION, available at <https://www.itu.int/osg/spu/wsis-themes/Access/BackgroundPaper/IS%20Principles.pdf> Accessed 23rd August, 2020

[85] Section 70A, Information Technology Act, 2000.

[86] Section 70B, Information Technology Act, 2000.

[87] Sidharth Deb, 'Towards a Cyber-Security Roadmap for Digital Payments: Best Practices and Recommendations', OBSERVER RESEARCH FOUNDATION, available at <https://www.orfonline.org/wp-content/uploads/2019/04/ORF_Report_Roadmap-Digital-Payments-.pdf> Accessed 1st September 2020.

[88] Saikat Datta, 'Defending India's Critical Information Infrastructure', INTERNET DEMOCRACY PROJECT, available at < https://internetdemocracy.in/wp-content/uploads/2016/03/Saikat-Datta-Internet-Democracy-Project-Defending-Indias-CII.pdf> Accessed 1st September, 2020.

[89] Karan Saini, Pranesh Prakash, et al, 'Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India', CENTRE FOR INTERNET AND SOCIETY, available at <https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf/view> Accessed 1st September, 2020.

sharing information.[90] Furthermore, the current framing of the Act and the related Rules on designation of sectors as CIIs lends to an over-inclusion under broad sectors which are designated as CIIs. [91] As the government overhauls the data protection framework, many coordination and harmonisation challenges are further expected to arise. For instance, the Data Protection Authority (DPA) set up under the Personal Data Protection Bill 2019 is also expected to oversee and respond to cyber security breaches, lending to expected overlaps between the DPA and existing authorities under the IT Act.[92] These must be rationalised in a reform of the IT Act.

- A detailed mapping of the IT Act and potential issues for reform is in **Appendix I** of this document. In respect of each of these issues **and other novel issues** identified over the course of research, the proposed ITDR Act should be expected to:[93]

    1. **Establish the scope of rights** guaranteed and recognised in relation to the digital ecosystem.

    2. **Defines standards** for each issue in compliance with these rights.

    3. **Define the obligations** of state authorities and private actors to effectuate and safeguard these rights.

    4. **Design institutional arrangements** to divide responsibility among state authorities.

    5. **Establish a right to remedy** to enforce these rights.

III. Identification of rule-making procedures and enforcement mechanisms

- The present design of rule-making powers in the IT Act offers the executive with near-unbridled powers to make subordinate legislation, without specifying a procedure for the same.[94] Instead, a **procedure for the exercise of this power** should be identified in the new legislation to govern all future rule-making under the ITDR Act. These rules would also be required to comply with the broad rights set out in the Act, further canalising this power, and placing safeguards on all future rule making. Some of the mechanisms that merit discussion in this regard are:

    - ***Stakeholder consultation in defined formats***
      The participation of various stakeholders can be mandated by making consultations with the stakeholders a mandatory pre-condition to the enactment of any delegated legislation. To prevent this requirement from being subverted, the format of such consultation can be defined, except for some emergency situations. This can take the form of issue-specific advisory groups and committees which provide recommendations on various issues.[95] Additionally, a delegated

[90] Karan Saini, Pranesh Prakash, et al, 'Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India', CENTRE FOR INTERNET AND SOCIETY, available at <https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf/view> Accessed 1st September, 2020.

[91] Sidharth Deb, 'Towards a Cyber-Security Roadmap for Digital Payments Best Practices and Recommendations', OBSERVER RESEARCH FOUNDATION, available at <https://www.orfonline.org/wp-content/uploads/2019/04/ORF_Report_Roadmap-Digital-Payments-.pdf> Accessed 1st September 2020.

[92] Sidharth Deb, 'Towards a Cyber-Security Roadmap for Digital Payments Best Practices and Recommendations', OBSERVER RESEARCH FOUNDATION, available at <https://www.orfonline.org/wp-content/uploads/2019/04/ORF_Report_Roadmap-Digital-Payments-.pdf> Accessed 1st September 2020.

[93] Elizabeth Garrett, 'The purposes of framework legislation', 14 JOURNAL OF CONTEMPORARY LEGAL ISSUES, 717 (2004)

[94] Section 87(1), Information Technology Act, 2000.

[95] While the formation of advisory groups and committees helps bolster stakeholder consultation processes, the formation of permanent groups in this regard may have the effect of turning them into exclusive conduits for stakeholder consultation, and in the process, exclude avenues for public participation. *See* Jeanette Hoffman, 'Multi-stakeholderism in Internet Governance: putting a fiction into practice', 1

legislation can be deemed to be legally invalid if it does not conform to stakeholder consultation in the defined format.

- ***Mandatory time-periods for stakeholder consultation***

  To ensure that stakeholder consultation happens in an effective manner which allows the representation of many views, the time periods for this process can be placed in the legislation itself, thereby operating as strict controls on the way in which the stakeholder consultation process is conducted.

- ***Review of any use of emergency rule making powers***

  While it may be necessary to provide some emergency powers, given that all situations in which rule-making powers may need to be exercised cannot be foreseen, there should be appropriate provisions to enable an effective review of any exercise of emergency powers under the Act.

- ***Creation of enforcement authorities***

  The robust enforcement of the legislation would depend on the institutional mechanisms that are developed to administer and enforce it. The establishment of institutions for the purposes of coordination, collective action and enforcement of the legislation is necessary to operationalise the ITDR Act. This may entail the **creation of enforcement authorities**. This would be required both for specific issues like content regulation,[96] cybersecurity,[97] control over certifying authorities[98] as well as for the general enforcement of other provisions of the ITDR Act. The creation of these authorities would also enable the Act to effectively and precisely allocate responsibility for various issues, as mentioned above.

JOURNAL OF CYBER POLICY (2016) ("Discussing some of the criticisms of the Internet Governance Forum as a multi-stakeholder advisory group")

[96] *See* Info-communications Media Development Authority Act 2016 [Singapore]; 'Britain to create regulator for Internet content', THE NEW YORK TIMES, available at <https://www.nytimes.com/2020/02/12/technology/britain-internet-regulator.html> Accessed 23rd August, 2020

[97] Section 70B, Information Technology Act, 2000.

[98] Section 18, Information Technology Act, 2000.

IV. Way forward

- Having established the need for, purpose of and contours of a framework legislation for information technology, the next step is to examine the substantive content of the rights, obligations, and structures that such a legislation would establish. This will involve an analysis of information technology as it relates to our social, economic, and political environment, as well as an analysis of the effectiveness of potential measures to regulate information technology use.

- The formulation of a set of digital rights would be necessary for the institutionalisation of these rights. This would require consolidation of existing jurisprudence on individual rights in the digital environment, as well as a mapping of novel manifestations of constitutional entitlements in the digital sphere. This exercise must pay heed to emerging issues of internet access and technological exclusion and should extend to both economic as well as civil and political rights. Importantly, any formulation of these rights should be capable of limiting the actions of both State and private entities, thereby placing the individual at the centre of any such legislation, empowering the individual and safeguarding their interests.

- The issues mapped in this document represent the first step towards consolidation of the scope of the IT Act. This exercise must be exhaustively conducted to be able to precisely identify the scope of regulation of any new legislation. This endeavour must be supplemented with a conceptual study of what this scope should normatively be – by analysing the various harms, functions, and effects that a new legislation is envisaged to regulate.

- The development of consensus on, and precise identification of the following, would represent progress towards concretising the vision of the ITDR Act. This forms the next step in this inquiry:

    - Formulation of a charter of digital rights and fundamental governance principles for the digital environment;

    - An enumeration of the substantive issues which should be regulated by the Act; and

    - An identification of the rulemaking procedures and enforcement mechanisms necessary to operationalise the Act

Appendix I: Consolidation of issues under the IT Act

Broad scope/issue	Description	Relevant provisions
Recognition of electronic signatures	Use of digital/electronic signature for authentication of electronic records	1. Section 3, IT Act. 2. Section 3A, IT Act. 3. Digital Signature (End entity) Rules, 2015 4. Information Technology (Certifying Authorities) Rules, 2000
	Legal recognition of electronic/digital signatures	1. Section 5, IT Act.
	Use of electronic signatures by governmental agencies	1. Section 6, IT Act. 2. Information Technology (Use of Electronic Records and Digital Signature) Rules, 2004
	Security procedures in respect of electronic signature	1. Section 15, IT Act. 2. Section 16, IT Act. 3. Information Technology (Security Procedure) Rules, 2004
	Digital/Electronic Signature Certificate and the regulation of its issuance, suspension and revocation	1. Chapter VII, IT Act. 2. Digital Signature (End entity) Rules, 2015 3. Information Technology (Certifying Authorities) Rules, 2000 + 2015 Amendment
	Penalty for false/fraudulent publication of electronic signature certificates	1. Section 73, IT Act. 2. Section 74, IT Act.
	Regulation of the Controller and Certifying Authorities	1. Chapter VI, IT Act. 2. Section 68, IT Act. 3. Section 82, IT Act. 4. Section 89, IT Act. 5. Information Technology (Certifying Authorities) Rules, 2000 + Amendments (2003, 2004, 2009, 2011, 2015) 6. Ministry of Communications and Information Technology, Department of Electronics and Information Technology, Controller of Certifying Authorities, Director (Finance and Administration) Recruitment Amendment Rules, 2013
	Obligations of the subscriber	1. Chapter VIII, IT Act.
Recognition of electronic documents	Authentication of electronic records	1. Section 3, IT Act. 2. Digital Signature (End entity) Rules, 2015
	Legal recognition of electronic records	1. Section 4, IT Act.
	Use of electronic records by governmental agencies	1. Section 6, IT Act. 2. Information Technology (Use of Electronic

		Records and Digital Signature) Rules, 2004
	Retention of electronic records	1. Section 7, IT Act. 2. Section 9, IT Act.
	Audit of electronic records	1. Sections 7A, IT Act. 2. Section 9, IT Act.
	Publication in the Electronic Gazette	1. Sections 8, IT Act. 2. Section 9, IT Act.
	Validity of electronic contracts	1. Section 10A, IT Act.
	Attribution, acknowledgement and dispatch and of electronic records	1. Chapter IV, IT Act.
	Security procedures in respect of electronic records	1. Section 14, IT Act. 2. Section 16, IT Act. 3. Information Technology (Security Procedure) Rules, 2004
Regulation of electronic service delivery	Authorization of service providers to deliver electronic services	1. Section 6A, IT Act. 2. Information Technology (Electronic Service Delivery) Rules, 2011
	Notification of delivery of electronic services	1. Information Technology (Electronic Service Delivery) Rules, 2011
	Repository of electronically signed electronic records used by government authorities	1. Information Technology (Electronic Service Delivery) Rules, 2011
	Responsibility of service providers in respect of financial management and accounting	1. Information Technology (Electronic Service Delivery) Rules, 2011
	Audit of information systems and accounts of service providers	1. Information Technology (Electronic Service Delivery) Rules, 2011
Confidentiality and security of computer resources	Protection of confidential information	1. Section 72, IT Act 2. Section 72A, IT Act
	Security procedures for electronic documents and signatures	1. Section 16, IT Act 2. IT (Security Procedure) Rules, 2004
	Penalties for unauthorised access or damage to computer resources	1. Section 43, IT Act
	Compensation for failure to protect personal data and secure it in compliance with reasonable security procedures and practices prescribed	1. Section 43A, IT Act 2. IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
Cybercrime, offences and penalties	Offences related to unlawful access to, and tampering with electronic documents and computer resources, and dishonestly receiving stolen computer resources.	1. Section 65, IT Act 2. Section 66, IT Act 3. Section 66B, IT Act
	Offences related to identity theft and cheating by personation using a computer resource	1. Section 66C, IT Act 2. Section 66D, IT Act.
	Offences relating to transmission and publication of obscene content,	1. Section 66A, IT Act[99] 2. Section 66E, IT Act

[99] This section was struck down by the Supreme Court of India in Shreya Singhal v. Union of India, (2015) 5 SCC 1, for violating the right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India as the language employed by the section was vague and did not conform with the reasonable restrictions under Article 19(2) of the Constitution.

	image of "private area" without their consent, and material containing sexually explicit acts, and depicting children in sexually explicit acts.	3. Section 67, IT Act 4. Section 67A, IT Act 5. Section 67B, IT Act.
	Offences pertaining to cyber-terrorism	1. Section 66F, IT Act
Content Regulation	Offences related to content on the Internet	1. Section 67, IT Act 2. Section 67A, IT Act 3. Section 67B, IT Act
	Governmental powers to block content on the Internet	1. Section 69A, IT Act 2. IT (Procedure and safeguards for blocking for access of information by public) Rules, 2009
	Content regulation by intermediaries	1. Section 79, IT Act 2. IT (Intermediary Guidelines) Rules, 2011
Regulation of intermediaries	Mandate to remove content upon notification by the government, or via judicial orders, and following due diligence requirements specified.	1. Section 79, IT Act 2. IT (Intermediary Guidelines) Rules, 2011
	Obligations for preventing unauthorised monitoring and collection of traffic data, and cooperating with the relevant authorities	1. Section 69B, IT Act 2. IT (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009
	Registration and compliances for cyber cafes	1. Section 79, IT Act 2. IT (Guidelines for Cyber Cafe) Rules, 2011
	Punishment for non - compliance with orders for information preservation and retention orders, content blocking, decryption and interception	1. Section 67C(2), IT Act 2. Section 69(4), IT Act 3. Section 69A(3), IT Act
	Retention of information by intermediaries and regulation of digital locker facilities	1. Section 67C, IT Act 2. IT (Preservation of Information by Intermediaries providing Digital Locker Facilities) Rules, 2016
Law enforcement assistance	Powers to order decryption and interception of communications	1. Section 69, IT Act 2. IT (Procedure and safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
	Powers to block access to information in national interest	1. Section 69A, IT Act 2. IT (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009
	Powers to order content takedowns by intermediaries	1. Section 79, IT Act 2. IT (Intermediary Guidelines) Rules, 2011
Cybersecurity authorities and powers related to cybersecurity	Government powers to call for computer traffic information for detecting cyber security threats and plugging breaches.	1. Section 69B, IT Act 2. IT (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009
	Protection of critical information infrastructure (CII), offences related to compromise of CII, appointment	1. Section 70, IT Act 2. Section 70A, IT Act 3. Section 66F, IT Act

	of nodal agency (National Critical Information Infrastructure Protection Centre, notification of certain computer resources as Protected Systems (e.g.CIDR under Aadhaar)	4. IT (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 5. IT (Information Security Practices and Procedures for Protected System) Rules, 2018
	Appointment of Computer Emergency Response Team as the nodal agency for computer emergency response for cyber security incidents	1. Section 70B, IT Act 2. IT (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 3. IT (Salary, Allowances and Terms and Conditions of Service of the Director General, Indian Computer Emergency Response Team) Rules, 2012.
	Power to prescribe methods or modes for encryption.	1. Section 84A, IT Act
Miscellaneous	Jurisdictional scope of the Act	1. Section 1(2), IT Act 2. Section 1(4), IT Act 3. Section 81A, IT Act 4. Schedule I, IT Act
	Recognition of electronic evidence and appointment of examiners	1. Chapter XII A, IT Act
	Powers to make rules regulations, and give directions under the Act	1. Section 10, IT Act. 2. Section 86, IT Act 3. Section 87, IT Act 4. Section 89, IT Act 5. Section 90, IT Act 6. Section 83, IT Act
	Authorities under the Act - Adjudicating Officer, Appellate Tribunal, Controller of Certifying Authorities and Advisory Committee	1. Section 46- 47, IT Act 2. IT (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003. 3. Chapter X, IT Act 4. Section 88, IT Act 5. Chapter VI, IT Act 6. Section 68, IT Act 7. Section 82, IT Act 8. IT (Certifying Authorities) Rules, 2000
	Nature of offence, residuary penalty, and offences by companies	1. Sections 77-78, IT Act 2. Section 45, IT Act 3. Section 84B, IT Act 4. Section 84C, IT Act 5. Section 85, IT Act
	Police powers to investigate offences	1. Section 80, IT Act