Practise what you preach

Pranesh Prakash

2012-04-26

Indian Express

Abstract

The only way to fix India's IT laws is to change the way they are made

---

Laws in India relating to the Internet are greatly flawed. The only way to fix them would be to fix the way they are made. The Cyber-Laws and E-Security Group in the Department of Electronics and Information Technology (DEIT, 'DeitY' according to their website) has proved incapable of making balanced,informed laws and policies. The Information Technology (IT) Act is filled with provisions that neither lawyers nor technologists understand.

The rules drafted under Section 43A of the IT Act (on "reasonable security practices") were so badly formulated that the government was forced to issue a "clarification" through a press release,even though the "clarification" was in reality an amendment and amendments cannot be carried out through press releases. Despite the clarification,it is unclear to IT lawyers whether the rules are mandatory or not,since Section 43A (the parent provision) seems to suggest that it is sufficient if the parties enter into an agreement specifying reasonable security practices and procedures. Similarly,the IT (Intermediary Guidelines) Rules (better referred to as the Internet Censorship Rules) drafted under Section 79 of the act have been called "arbitrary and unconstitutional" by many,including the member of parliament,P. Rajeev,who has introduced a motion in the Rajya Sabha to repeal the rules. These rules give the power of censorship to every citizen and allow him to remove any kind of material from the internet within 36 hours without anybody finding out. Last year,we at the Centre for Internet and Society used this law to get thousands of innocuous links removed from four major search engines without any public notice. In no case (including one where an online news website removed more material than the perfectly legal material we had complained about) was the content-owner notified about our complaint,much less given a chance to defend herself.

Laws framed by the Cyber-Laws Group are so poorly drafted that they are often misused. There are too many criminal provisions in the IT Act,carrying much graver penalties than those for comparable crimes under the Indian Penal Code. Section 66A of the IT Act,which criminalises "causing annoyance or inconvenience" electronically,has a penalty of three years (greater than that for causing death by negligence),and does not require a warrant for arrest. This

section has been used in the Mamata Banerjee cartoon case,and against former Karnataka Lokayukta Santosh Hegde. Section 66A imperils freedom of speech more than is allowable under Article 19(2) of the Constitution.

While Section 5 of the Indian Telegraph Act allows telephone tapping only if there is a public emergency,or in the interests of the public safety,the IT Act does not have any such condition,and greatly broadens the state's interception abilities. Section 69 of the IT Act allows the government to force a person to decrypt information,and might clash with Article 20(3) of the Constitution,which provides a right against self-incrimination. No publicly available governmental document suggests that the constitutionality of provisions such as Section 66A or Section 69 was examined.

Omissions by the Cyber-Laws Group are also numerous. The Indian Computer Emergency Response Team (CERT-In) has been granted very broad functions under the IT Act,but without any clarity on the extent of its powers. Some have been concerned that the powers granted to CERT-In to "give directions" on "emergency measures for handling cyber security incidents" includes the power of an "Internet kill switch",which Egypt exercised in January 2011. Yet,no rules have been framed for the functioning of CERT-In. The licences that the department of telecommunications gives the internet service providers requires them to restrict usage of encryption by individuals,groups or organisations to a key length of 40 bits in symmetric key algorithms (i.e.,weak encryption). The Reserve Bank of India mandates a minimum of 128-bit SSL encryption for all bank transactions. Rules framed by the DEIT under Section 84A of the IT Act were to resolve this conflict,but they haven't yet been framed.

All of this paints a very sorry picture. Section 88 of the IT Act requires the government,"soon after the commencement of the Act",to form a "Cyber Regulations Advisory Committee" consisting of "the interests principally affected or having special knowledge of the subject-matter" to advise the government on the framing of rules,or for any other purpose connected with the IT Act. This body still has not been formed,although it has been more than two years since the IT Act came into force. Justice Markandey Katju's recent letter to Ambika Soni about social media and defamation should ideally have been addressed to this body.

The only way out of this quagmire is to practise at home that which we preach abroad: multi-stakeholderism. This refers to the need to recognise that there are multiple stakeholders — government,industry,academia,and civil society — when it comes to internet governance,and not just the governments of the world. This idea has gained prominence since it was placed at the core of the "Declaration of Principles" from the first World Summit on Information Society in Geneva in 2003,and has been at the heart of India's pronouncements at platforms like the Internet Governance Forum. The DEIT's Internet Governance Division,which formulates India's international stance on internet governance,has long recognised that such governance must happen in an open and collaborative manner. It is time the DEIT's Cyber-Law Group,which formulates our national stance on internet governance,realises the same.

The writer is at the Centre for Internet and Society,Bangalore