www.naavi.org

ITA 2008 Rules to be presented in the Parliament

The rules notified under ITA 2008 on April 11, 2011 have evoked many comments and criticisms from Netizens, Companies, Media and others.

The set of four rules released were

a) Rule under Sec 43A- GSR 313(E)

b) Rule under Sec 79 for Intermediaries-GSR 314(E)

c) Rule under Sec 79 for Cyber Cafes-GSR 315(E)

d) Rule under Sec 6A -GSR 316 (E)

The notifications will now be placed in the Parliament during the current session and amidst the Lokpal and 2G scam discussions it is possible that the rules may go through without debate.

For the last few months, I have been drawing the attention of the Ministry of Communications and Information Technology (MCIT) on two specific issues namely the issue of removing sub rules 8(2), 8(3) and 8(4) in the notification regarding Section 43. I have also been corresponding on the appointment of a Chairman for CAT.

On the Section 43 rules, I have been receiving some response though I am yet to receive confirmation on the removal of the sub rules as suggested. On the CAT issue there is complete silence.

I will be drawing the attention of some of the Parliamentarians again through this article which will be individually notified to some of the relevant Parliamentarians so that some action can be taken in the Parliament.

Since most MPs are difficult to reach through e-mails, I request the readers to forward a copy of this article which will be available in PDF form for download to MPs they know. If some body can reach it to all the MPs I request them to do so.

Naavi

Rules under Sec 79 (Intermediaries):

The proposed rules under Section 79 is the one which has attracted the most of the media attention both in India and abroad. There have been a couple of articles in the American Press as well. In one of the recent such articles in Washington Post it was stated that an official of the MCIT has stated that the Government is willing to listen to dissenting views and could consider changes.

Though the Ministry is normally stubborn and does not relish changing its views, I hope this time it would be different since the objection is not from Indian observers or Indian media but from Washington Post. After all the Ministry must have different standards for Indian views and foreign views. I am therefore tempted to post my detailed views here with the hope that the MCIT has its eyes and ears open, a heart to respond, a head to swallow its pride and hands to act appropriately.

Section 79 of ITA 2008 is not a penal section under the Act. Penalty under the Act would arise on any person or a body corporate on account of other sections such as Sec 43, 43A, 65,66, 66A, 66B, 66C, 66D, 66E,66F,67, 67A, 67B, 69,69A, 69B, 70, 71, 72, 72A, 73, 74, 84B, 84 C etc. When an incident has occurred which can be brought under any of these sections and the person who is accused is otherwise an "Intermediary" as defined under the Act, then the provisions of Section 79 apply to provide him an opportunity to escape liability. For this purpose he needs to act in a manner which can be considered as "Exercising Due Diligence" and the said rules try to define such conditions as may be required to enable an "Intermediary" to escape liability.

The intermediary which is given such privilege includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

One of the aspects of due diligence that has attracted the criticism from public is the sub rule 3 (4) which states as follows:

"The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes"

Sub rule 3(2) referred to here states things such as

> a) belongs to another person and to which the user does not have any right to;
> (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in

any manner whatever
(c) harm minors in any way;
(d) infringes any patent, trademark, copyright or other proprietary rights;
(e) violates any law for the time being in force;
(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
(g) impersonate another person;

One of the contentions is that the descriptions of what not to do is too broad and leaves the scope for interpreting any content under this sub section.

Further the prescription that the Intermediary has to act within 36 hours of being brought to notice by the affected person and possibly disable the information makes the rule draconian.

Though the Government will claim that there is no "Compulsion" to remove the content and what is intended is only to respond within 36 hours and such response may even be a counter e-mail to the person responsible for the content to give his counter views it is possible for threatening notices to be sent to Intermediaries by advocates of the affected persons which can unnerve the business owners of the Intermediaries.

We have plenty of examples in India where even Courts have issued temporary injunctions on defamation suits without going into the merits of the case or giving an opportunity to the counter party to lodge his views. There are also cases where Courts not having jurisdiction for the relevant complaint also issuing a blind gag order. The MCIT in such cases has been found to have acted without a responsibility of its own and without even clarifying or seeking clarification from the Court issued implementation instructions based on such "Court Orders". Naavi.org has provided information on such issues earlier. There is the case of E2 Labs where the MCIT was duty bound to implede and oppose the order of the Delhi High Court to block zone-h.org but failed to do so. There is the case of CAT which has sat in judgment of such defamation suits and issued temporary injunctions when its jurisdiction was not clear. It is therefore considered that an influential advocate can get a Court order for blocking a website on any flimsy ground under the pretext of an interim order without the Court being able to go into the merits of the complaint.

In view of this situation, leaving the rules under Section 79 in its present form where not even a Court order is required for blocking of a content is a definite blow to the democratic status of India where "Freedom of Speech" is expected to be present.

It is acknowledged that Naavi.org would perhaps be one of the targets of some persons affected by its views. There will be many more public service "Intermediaries" who will be easily harassed with notices if rule 79 in its present form is allowed to go through.

The Intermediaries (Remember that many of them could be foreign agencies) are expected to report Cyber Security Incidents to CERT-In as a rule. Such Security incident is not limited to some specific

content which is a subject of dispute. How does the Government expect a foreign Intermediary to share its Cyber Security Incidents with the Indian Government as a matter of routine (As opposed to any query in respect of a lawful investigation of a crime) is beyond imagination. Having such impractical rules is a recipe for the rules to be junked by the community.

The only sensible portion of the law is that the Intermediary shall appoint a "Grievance Officer" and introduce a mechanism for grievance redressal. Posting if terms and conditions and obtaining consent from the person who posts the content that he will abide by that is also reasonable. The description of the offences under Sec 79 should be limited to "Any contravention of the provisions of ITA 2008" rather than giving a list of offences as provided under rule 3(2). The Cyber security incident reporting should be limited to specific queries received from a law enforcement agency through a proper process.

As regards the responsibility for removing the content the owner of an Intermediary cannot be made a judge on what content is violative of the law. Hence on receipt of a digitally signed e-mail from the affected person a decision cannot be taken by the Intermediary.

It is therefore proposed that the only action that the Intermediary is required to take should be "To post the objection raised by the affected person as a rejoinder to the earlier content". At present most blogs provide for comments to be posted. This does not require a digital signature. Some times the authors regulate the comments and accept some and reject some. The Intermediary can only take away the right of the person posting the content to reject a comment placed by the affected person. In other words, the affected person can place his views as a part of the comment which can be done instantaneously in most cases. If the comments are disabled or moderated and not posted within say 24 hours then the affected person can file a complaint with the Grievance officer and he shall ensure that the objections are posted prominently under the same article which may contain the objectionable content.

If the "Intermediary" holds any sensitive personal information, obligations regarding the same is already covered under the rules under sec 43A and there is no need to repeat it under rules for Sec 79.

Thus there is scope for a major simplification of the rule under Section 79. I have been personally drafting Terms and Conditions for Intermediaries and have always included the clause regarding "Users not to violate any provisions of ITA 2008" and that "An Ombudsman shall be appointed by the Intermediary".

Hence if the Government of India wants some specific suggestion on how this notification should be revised and simplified, I would be able to provide the necessary support.

Rules under Sec 79 (Cyber Cafes):

The proposed rules for Cyber Cafes suffer from the fact that it is too complicated for the target community and has the indirect effect of closing down the industry as we know it today. It is also an incomplete rule requiring further rule making at the State Government level. There is also an impression

that this rule may infringe on the powers of the State Government for law and order maintenance in the State.

We must remember that a Cyber Cafe is also an "Intermediary" hence the obligations under Section 79 and the rules framed there in for "Intermediaries" already apply to Cyber Cafes. If the Government thought it was necessary to have a separate set of rules for Cyber Cafes, they should have first thought of removing "Cyber Cafes" from the definition of "Intermediaries". Similarly the notification under Section 6A [GSR 316(E)] defines the "Electronically Enabled Kiosk" for which the rules under 6A is made applicable as "Cyber Cafe as defined in ITA 2008".

The logic of this multiple legislatory onslaught on the poor Cyber Cafe owner defies logic unless this is a move to reserve the industry only for corporate Cyber Cafes.

It is necessary for us to appreciate that Cyber Cafes have done yeoman service to the Country in popularizing Internet at a time when Internet access was expensive. Now with Broadband connectivity being available everywhere at affordable prices, Cyber Cafes have a tough time to attract customers and have to device innovative service offerings to retain their clientele. Most Cyber Cafes double up as photocopy centers. In Tamil Nadu Cyber Cafes have been used for delivery of E Government services. Most Cyber Cafes are managed by individuals and provides a lively hood for them.

There is however a need for regulating Cyber Cafes since they can be and are used by criminals for their activities. This is mostly a "Law enforcement Issue" and hence regulation of Cyber Cafes is primarily a responsibility of the Police. To the extent Cyber Cafes operate in Cyber Space, the Central Government can take upon itself the responsibility for regulation of the Cyber Cafes but the need of the State Government to be the main instrument of regulation of Cyber Cafes cannot be undermined.

In this context the Cyber Cafe regulation should have been in the form of an "Advisory" and provided a "Template for State Regulation" so that there would be uniform legislation across the Country.

Instead the Government has opted for an independent rule which infringes on the State subject and can be considered as violative of the principles enshrined in the Constitution of India.

The second objectionable aspect of the rule is that it is not complete without the formation of the State level "Cyber Cafe Registration Agency" with an appropriate process for registration, de-registration and monitoring.

In case the GOI wants to take up the responsibility for Governing Cyber Cafes across the Country, it is open to them to start a new Central Agency as proposed in the ESD Bill for E Government Service Delivery and notify a complete rule including the registration rule.

The third objection that can be raised on the Cyber Cafe regulation is that it is too complicated for a normal cyber cafe. The rule for maintaining a visiting register and noting down the ID card details are reasonable. The rule regarding maintaining anti Virus and desktop security systems is also reasonable.

It must however be remembered that if the Cyber Cafe is required to maintain the personal information of the users they are exposed to the responsibilities under Section 43A and 72. The rule does not provide a work around for this.

The rules also mandate that "Cyber Cafe shall prepare a monthly report of the log register showing date-wise details on the usage of the computer resource and submit a hard and soft copy of the same to the person or agency as directed by the registration agency by 5th of the next month". (Log Register here refers to the visitor's register).

If a monthly report is being submitted the need to maintain the register for one year becomes redundant. However the rule requires both.

Additionally the Cyber Cafe is required to capture the "History of Websites visited" and "Logs of Proxy Server" and the attention of the Cyber Cafe owner is drawn to the auditing and logging process referred under CISG-2008-1 of the CERT IN. This requirement clearly indicates that the persons who drafted the rule did not have any idea of the profile of Cyber Cafe owners in India and whether they can understand a document such as CISG-2008-1. It would be interesting for the Cyber Cafe Association somewhere to organize a meeting of Cyber Cafe owners and invite the official responsible for drafting this rule to come and explain to them the document CISG-2008-1.

Rule 5(1) as well as 5(5) talk about maintaining the log register for one year. It appears one was meant for the Visitor's register and the other for the log of records under rule 5(4) including the History of websites and system log records.

Again the department appears to have not taken into account what is the volume of such information that would be developed or the costs involved if these records are to be stored for one year with an appropriate back up and reasonable security.

The department failed to see any alternatives for such a measure which imposes too much of a burden on the Cyber Cafe and is likely to be simply ignored.

The biggest beneficiary of this suggestion is creation of an opportunity for the Cyber Cafe Inspector to collect a regular charge from every Cyber Cafe under his jurisdiction to look the other way. Perhaps a "Strong Lok Pal" will be required to ensure that the rule does not become an instrument of harassment for the Cyber Cafe owners.

The most appropriate option for the Government is therefore to withdraw this notification completely and constitute a committee of three or four state IT Secretaries and request them to draft a model Cyber Cafe regulation for the States. Naavi has already placed more comprehensive suggestions for drafting a Cyber Cafe regulations copies of which are available with MCIT and also the Karnataka State Government. If required the draft regulation can once again be sent to the proposed committee of IT Secretaries for their information.

I presume that this rule can be challenged in a Court of Law for being unreasonable and infringing on the State's powers.

Rules under Sec 43A (Reasonable Security Practices):

The rule which has really shaken up the Indian Corporate sector is the rule under Section 43A which defines "Sensitive Personal Information" and "Reasonable Security Practices".

Under Section 43A, any Body Corporate (any person other than an individual) handling "Sensitive Personal Information" is required to adopt "Reasonable Security Practices" to avoid liabilities under the section. The liabilities may arise when a person whose sensitive personal data is not adequately protected can claim compensation for a "Wrongful harm".

Part of the rule is devoted to reproducing the well known principles of Privacy such as Minimum Collection, Purposeful Collection, default Opt-Out facility, appropriate disclosure to the data subject, need to know disclosure within the organization, destruction after requirement is complete etc.

The "Sensitive Personal Information" is defined to include Password, financial information, health information, sexual orientation, biometric information etc.

The biggest controversy regarding Section 43A notification arises out of Rule 8 on "Sensitive Personal Information". Naavi has been corresponding with the MCIT over the last three months to convince them that the rules give a wrong impression to the public that

a) ISO 27001 audit is mandatory for compliance of Section 43A and has to be renewed once a year.

b) Companies who have already completed ISO 27001 audit are not required to do any thing else at present to comply with Section 43A

Naavi has objected to the provisions of Sub rule 8(2), 8(3) and 8(4) and demanded that they be dropped. He has alleged that the rules has been written in such a manner as to make it appear that ISO 27001 mandatory and this is neither desirable nor legal. He has pointed out that such a rule results in the following

a) One cannot fully understand the provisions of the rules under Sec 43 A (a law of the land in other words) without purchasing a copy of the specifications of ISO 27001 which costs Rs 7000/- to be paid in foreign exchange to a foreign body. If 120 crore Indians need to know the law of the land all of them have to incur this expenditure compulsorily. The financial benefit transferred to the foreign agency is of the order of the value of the 2G scam and amounts to a "Tax" on the community.

b) It is inappropriate for the Government of India to include in its statutory law a certification that "If you are ISO 27001 certified you are compliant with Indian Law". This provides a commercial advantage to ISO 27001 organization and its implementing agencies and passes on

financial benefits. The estimated benefit to the ISO 27001 community in getting ISO 2701 audits conducted each year may amount to Rs 3 lakh per company for an estimated 10 lakh companies (Rs 30,000 crores per annum)

c) ISO 27001 audits donot cover ITA 2008 audit as a default and hence all companies who are presently certified for ISO 27001 or may be certified in future cannot be considered as being compliant with section 43A of ITA 2008. Hence sub rule 8(4) will turn out to be a controversy.

Naavi has queried with MCIT on the ISO 27001 issue and has been informed as follows by Mr Prafulla Kumar, Director, MCIT dated 11th July 2011.

> 4. Rule 8 do not mandate implementation of ISO 27001 standard exclusively. Body corporate are free to adopt and implement other codes of best practices agreed by the Industry Associations or an entity formed by Industry Association. Thus the presumption that body corporate will have to necessarily procure ISO27001 document is not in order. They can adopt other codes of best practices suiting to their nature of business.

Department says that any Body Corporate can chose any other framework if it desires. However since any other framework requires an approval from the department through a Gazette notification, it would be as good as notifying another rule under Section 43A.

Hence one can presume that the department wants the public to think that ISO 27001 is the only security framework that can be used. If the department does not want this misconception, then it is necessary for MCIT to remove the sub rules 8(2), 8(3) and 8(4).

Rules under Sec 6A:

For some time before April 11, 2011, the e-Governance department of MCIT was in the process of drafting the E Services Delivery Bill (ESD Bill). The release of the rules under Section 6A addressed the same issues that ESD Bill tried to address. The latest draft of ESD Bill has now deleted many of the overlapping provisions and focused only on making delivery of E Governance service mandatory (Overriding Section 9 of ITA 2008) and developing an administrative infrastructure for management of delivery of electronic services. It was strange that two departments of the same Ministry were trying to pass legislation on the same matter.

It is preferable that MCIT resolves the differences between the e-Governance department and the Cyber Law department before the rules under Section 6A is pushed through the Parliament. Afterwards ESD Bill can be further modified to incorporate any issue which is presently addressed by rules under Section 6A and not addressed by ESD Bill.

In summary therefore it is recommended that rules under Sec 79 for Cyber Cafes and Rules under Section 6A may be withdrawn and Rules under Section 43A and 79 (Intermediaries) are modified as suggested.

The Issue of Appointment of CAT Chairman:

The issue of appointment of CAT Chairman is another issue that the undersigned has been pursuing for quite some time. By not appointing either a replacement for the retiring Chairman nor giving an extension to the current Chairman, the MCIT has ensured that all the work in CAT has come to a standstill and victims who were hoping for judgments after prolonged agony of pursuing the cases are now left to wait for Mr Kapil Sibal to get some time to look into this file amidst attending to 2G scam and Lokpal Bill requirements.

It is also possible that just like the CAT Chairman retiring before delivering the judgments, Mr Kapil Sibal may demit office before filling up the vacancy in CAT and leave the decision to a future Minister. If any midterm elections are announced, then every one would be busy in the election work and the appointment of CAT Chairman will get delayed until the next Government is in place. In case the Government has any semblance of sympathy on the hapless victims of Cyber Crime who are reeling under the injustice of delay in the dispute resolution it is necessary for the Government to take a quick decision in this matter immediately.

Naavi

July 15, 2011