National Consultation on enforcement of Cyber Law

(New Delhi- January 31, 2010)

Address by Hon'ble Sh. K.G. Balakrishnan, Chief Justice of India

---

Shri M. Veerappa Moily (Union Minister for Law and Justice)
Justice Altamas Kabir,
Justice Rajesh Tandon (Presiding Officer, Cyber Regulations Appellate Tribunal)
Sh. Goolam E. Vahanvati (Attorney General for India)
Dr. S. Sivakumar,
And Ladies and Gentlemen,

I am happy to be present here for the inaugural session of this national consultation for the enforcement of Cyber Law. As you are well aware, the objective behind organizing this programme is to devise a National Policy and Action Plan for improving awareness about this branch of law amongst judges, prosecutors and investigators. Therefore, it was felt that it was necessary to reach out to those at the helm of the Legal Services Authorities, the State Judicial Academies, the Director-Generals of Police in the various States as well as prosecuting agencies.

The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others. However, the means that enable the free flow of information across borders also give rise to a worryingly high incidence of irresponsible behaviour. Any technology is capable of beneficial uses as well as misuse. It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become tools of exploitation and harassment.

The Information Technology Act, 2000 addressed some basic aspects such as the legal recognition of electronic records and digital signatures for the purpose of entering into contracts and presenting evidence. However, substantial legal questions have arisen in many contexts. The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. Websites are created and updated for many useful purposes, but they can also be used to circulate offensive content such as pornography, hate speech and defamatory materials. In many cases, the intellectual property rights of authors and artists are violated through the unauthorized circulation of their works. There has also been an upsurge in instances of financial fraud and cheating in relation to commercial transactions conducted online.

Furthermore, the digital medium provides the convenient shield of anonymity and fake identities. Errant persons become more emboldened in their offensive behaviour if they think that they will not face any consequences. In recent years, there have been numerous reports of internet users receiving unsolicited e-mails which often contains obscene language and amounts to harassment. Those who post personal information about themselves on job and marriage websites or social networking websites are often at the receiving end of 'cyber-stalking'. Women and minors who post their contact details become especially vulnerable since lumpen elements such as sex-offenders can use this information to target potential victims.

In many cases, images or videos are created without the consent of the persons involved and they are unscrupulously circulated for commercial gain. A routine practice is the morphing of the images of well-known persons into pornographic content. Such practices are a blatant invasion of privacy as well as an attack on an individual's dignity.

However, there are inherent difficulties in using criminal laws to clamp down on them.

In theory, statutory provisions dealing with 'obscenity', 'defamation', 'cheating' and 'copyright infringement' are appropriate for proceeding against the perpetrators. Nevertheless, there are several hurdles in identifying the perpetrators in the first place. Criminal laws usually operate over a defined territorial jurisdiction but the content of websites can be created and uploaded anywhere in the world. Even when the source of offensive material is located, the police will face several practical difficulties in proceeding against perpetrators located in foreign jurisdictions. Even with respect to perpetrators in a local jurisdiction, there are problems on account of the structure of the flow of information over the internet. End-users can post content through fake identities and proxy server locations to misguide the investigating agencies.

The government can place bans on websites that exclusively circulate pornography and hate speech. However, it would not be right to place blanket bans on all categories of websites. It is also important to distinguish between intermediaries such as Network Service Providers, website operators and individual users for the purpose of placing liability for wrongful acts. Liability cannot be mechanically placed on internet intermediaries when it is specific individuals who engage in reprehensible conduct. That would be comparable to punishing the persons who build roads for the rash and negligent driving of other persons who operate vehicles on those roads.

This distinction between intermediaries and end-users is important because in many cases websites that ordinarily post acceptable material also allow users to circulate content on their own. This trend of relying on user-generated data has become prominent since it enables quick

updates on relevant information. However, it is quite possible that end-users may post offensive content without the knowledge of those who run the particular website or online forum. The investigators need to stay abreast with the latest developments in web-based applications so that they can quickly identify the actual perpetrators instead of going after an intermediary.

The Information Technology Act was amended a few months ago and Section 79 now provides a defence for 'Network Service Providers' who can demonstrate that they were not aware of the offensive content circulated through their services. While the limitation of liability was necessary to ensure that companies are not discouraged from providing internet access, the original problem has not been solved. More and more persons are being victimized through the digital medium and it is our moral responsibility to tackle the misuse of information technology.

Our legislation does try to account for some of these questions, but with the constant development of newer tools and technologies, the regulatory bodies must keep up. Ideally, we should strive for a balance between the interests of the service providers and the end-users. However, the content of such rules and regulations may result in disputes from time to time. The Cyber Regulations Appellate Tribunal (CRAT) has been established to hear and decide such disputes. Hence, the composition of this Tribunal should reflect the technological and judicial expertise needed to resolve such disputes. It is needless to say that those who serve on the tribunal need to be familiar with the latest developments in the field of Information Technology (IT) while also being alert to policy concerns and the need to ensure the free flow of information in society. Democratic values such as 'freedom of speech and expression', 'freedom of association' and the 'freedom to pursue an

occupation, business, profession or trade' need to be protected in the online domain as well.

There are of course many other legal questions that have arisen in respect of communications and transactions conducted through computers. It is heartening to see that many of the law colleges have introduced specialised courses dealing with this area. However, the immediate priority is to ensure that our investigators, prosecutors and judges become familiar with the various Information Technology (IT) related issues. With these words, I hope that this consultation programme will lead to some tangible outcomes.

Thank You!

***