Perry4Law
An Exclusive Techno-Legal Corporate, IP & ICT Law Firm

New Delhi, India

Cyber Law Trends And Developments Of India 2013

In continuation of the Cyber Law Trends and Development in India, Perry4Law and Perry4Law's Techno Legal Base (PTLB) are once again discussing the Cyber Law Trends and Development in India 2013. Some of the significant Trends and Development in this field in 2013 are as follows:

(1) Cyber Law Due Diligence: Cyber Law Due Diligence Requirements in India are neglected by various stakeholders. This is a serious issue that has not been resolved by Indian Government in the year 2013. Indian Government remained indifferent while Cyber Law Due Diligence requirements were flouted by Telecom Companies, E-Commerce Websites, etc.

(2) Internet Intermediary Liability: Internet Intermediary Liability in India is closely related to the Cyber law Due Diligence Compliances. As many stakeholders failed to ensure Cyber Law Due Diligence Compliances, they violated the Information Technology (Intermediaries Guidelines) Rules, 2011 of India (PDF).

(3) Telecom Companies Violations: Tata Teleservices Limited (TTL) and Airtel are Violating Indian Cyber Law and Internet Intermediary Rules of India. Complaints against Tata and Airtel are already pending before the Department of Telecommunication and Telecom Regulatory Authority of India (TRAI).

(3) E-Discovery Requirements: The need for E-Discovery for Indian companies has significantly increased in the year 2013 and it would even increase further in the year 2014. The Cyber Law Non-Compliances have given rise to an increased demand for E-Discovery in India.

(4) Corporate Frauds In India: Corporate Frauds Investigations in India have become multi disciplinary in nature. Besides the traditional corporate frauds, now Cyber Crimes and Technology Frauds have also become part of Corporate Frauds Investigation in India.

(5) Indo American Cyber Crimes Cooperation: An Indo-American alert, watch and warn network for real time information sharing in Cyber Crime Cases has been established to deal with Cyber Crimes cases falling within Indian and American jurisdictions.

(6) Corruption And Technology Related Due Diligence: Besides Cyber Law Due Diligence, the scope of Indian and Foreign Corruption and Technology related due diligences in India has also increased. With the passage of Lokpal and Lokayuktas Act, 2013 by the Indian Parliament, a stress upon corruption free environment has been made. Even Central Government permission is not required by CBI anymore to prosecute senior bureaucrats for corruption cases monitored by Supreme Court of India.

(7) Cyber Harassment And Cyber Stalking: Cases of Cyber Harassment and Cyber Stalking have increased in India. Websites like OLX is becoming a breeding ground for Cyber Harassment and Cyber Stalking. Further, allegations of selling stolen goods were also leveled against OLX.

(8) E-Commerce Compliances: Websites providing E-Commerce services in India are not complying with Indian Laws. The e-Commerce Websites must be regulated in India as they are operating with great disregard to Indian Laws. Although Indian Government has assured that E-Commerce in India would be regulated by comprehensive guidelines yet till date no such sign has been shown by the Government.

(9) Legality Of Bitcoins: The Bitcoin craze has finally started fading away as the Reserve Bank of India (RBI) issued a Warning Advisory against use of Bitcoins in India citing Cyber Security and Legal Risks. The Enforcement Directorate (ED) also searched Seven Digital Cash LLP office and website for selling and buying Bitcoins in India. The Legality of Bitcoins in India was always in doubts. Many countries like China, France, Thailand, Norway, etc have either regulated the use of Bitcoins or they have completely banned them in their jurisdictions.

(10) Conflict Of Laws In Cyberspace: Another problem that Indian Government is not willing to resolve pertains to Conflict of Laws in Indian Cyberspace. For long Companies like Google, Facebook, etc are violating Laws of India. Indian Government has not taken a tough stand against such Foreign Companies that although operating in India for profit yet are not complying with Indian Laws. For instance, G-Mail is abetting and encouraging commission of various Cyber Crimes in India yet Indian Government has allowed it to operate so far.

(11) E-Mail Policy Of India: There is no operational E-Mail Policy of India. The Delhi High Court is analysing E-Mail Policy of India and complaint mechanism to Facebook. The Delhi High Court has also directed Central Government to issue Notification regarding Electronic Signature under Information Technology Act 2000. An Advisory by Maharashtra Government to use Official E-Mails has already been issued. Even an E-Mail Policy of India is in pipeline.

(12) Cyber Crimes And Wildlife: Cyber Criminals are not leaving any opportunity to indulge in Cyber Crimes in India. The Cyber Criminals tried to crack the Iridium GPS Satellite Collar of a Tiger. The attempt to crack the collar was committed from Pune whereas the tiger with collar was located at a great distance at the tiger reserves of Madhya Pradesh. The Wildlife Crime Control Bureau (WCCB) has also recently traced at least 200 websites all over the country, which are being used by people to trade in animal parts. So the Cyber Crimes in India are evolving and Law Enforcement Agencies of India must be well equipped to deal with such Crimes.

(13) Child Porn Nuisance: Child Pornography in India is becoming a big nuisance. An Advisory (PDF) by Home Ministry of India on Preventing and Combating Cyber Crime against Children in India has also been issued. Recently Interpol helped India in tracking child porn surfers. We also need such Techno Legal Framework so that child pornography can be curbed to the maximum possible extent in India.

(14) Online Gambling In India: Although we have no dedicated Online Gambling Laws in India yet online gambling is fairly regulated in India under various Legislations. By indulging in gambling in online and offline manner, the concerned person or company would be violating the Laws of India. Many online gambling rackets were busted in the year 2013 and Indian Government must seriously consider regulation of Online Gambling in India.

(15) Online Pharmacies In India: Online Pharmacies in India are under regulatory scanner around the world, including India. Online sales of prescribed medicines in India are by and large unregulated and open for abuses. In fact, illegal and unregulated online sales of prescribed medicines in India are flourishing like a plague. Indian Government must give a serious thought to this area. Meanwhile, various stakeholders must understand various aspects of Telemedicine and Online Pharmacies Laws in India and their legal implications and liabilities.

(16) MLM Companies Frauds: Multi Level Marketing (MLM) frauds have significantly increase din India. Indian Government has even considered blocking of websites of MLM companies in India that are engaging in fraudulent behaviour. More clarity in this regard is needed.

(17) Civil Liberties Protection In Cyberspace: Civil Liberties Protection in Cyberspace is gaining importance in India and world wide Even at the United Nations (UN), Civil Liberties Protection in Cyberspace were considered. The United Nations even passed a resolution approving Right to Privacy in the Digital Age. However, India is in no mood of complying with that Resolution.

(18) E-Surveillance In India: E-Surveillance in India has increased tremendously despite the UN Resolution. India has launched Illegal and Unconstitutional Projects like Aadhar, Central Monitoring System (CMS), national Intelligence Grid (Natgrid), crime And Criminal Tracking Networks and Systems (CCTNS), Internet Spy System Network And Traffic Analysis System (NETRA), etc without any Parliamentary Oversight and Legal Frameworks. E-Surveillance, Civil Liberties Protection in Cyberspace and Conflict of Laws are some of the crucial issues that United Nations and India must consider on a priority basis.

(19) Internet Governance And India: In view of its growing Indian Cyber Security Concerns, India has decided to challenge the U.S. government's control over the Internet

and ensure that the trio of the U.S., Russia and China does not ignore India's concerns while developing an International Regime for Internet Governance. India will also push for storing all Internet Data and VOIP Services within the Country, besides ensuring control and management of servers.

(20) ICANN Free Domain Name Protection In India: The Policies and Agreements of Internet Corporation for Assigned Names and Numbers (ICANN) are in active violation of Indian Laws. Thus, Domain Name Protection in India must be free from ICANN's influence and must be judged independently of ICANN's Polices and Agreements.

There are many more aspects that we wish to discuss these Trends but due to the limited scope of this work, we are restraining from doing so. Perry4Law and PTLB hope that our readers would find this Trend useful.