CYBER CRIMES: THE INDIAN LEGAL SCENARIO

Maneela[*]

Crime is an act or omission, which is prohibited by the law. Cyber crime may be said to be an act which violates net etiquettes. Cyber crime is the latest and perhaps the most specialized and dynamic field in cyber laws. One of the greatest lacunae of this field is the absence of a set of comprehensive law anywhere in the world. Further the growth ratio of Internet and cyber law is not proportional, too. The idea of Internet was conceived in the early 60's while a code for its regulation was mooted in late 90's. This clearly brings about the reason for the complication of cyber crime. Any crime essentially consists of two elements namely, actus reus and mens rea. In the same way, cyber crime is also caused due to these two underlying factors—I. Actus Reus in cyber crimes; and II. Mens Rea in cyber crimes.

[*] Dr., Department of Law, D.A.V. (P.G.) College, Muzaffarnagar (U.P.), C.C.S. University, Merrut (U.P.), India. Research fields: Labour Laws and Cyber Laws.

INTRODUCTION

Since, the independence of India, i.e., August 15th, 1947, it has been struggling through to make its stand in the world. Many new technologies were brought and many new are still to be found. One such revolution was brought about by the introduction of the Internet, which is considered as the pool of knowledge. But who could think of the time when this rich source of knowledge will be misused for criminal activities.

There are many such disturbing activities that occurred in past and demanded for some rules and regulations urgently, some set definite patterns that can be put forward while carrying out any business transaction over the net, ranging from simple friendly e-mail to carrying out the whole set of work, without which it may go wild and beyond control and it can be used as a tool for the destruction of mankind. New forms and manifestations of cyber crimes are emerging every day. Therefore, to control cyber crimes new legislative mechanisms are required.

The largest challenge to the law is to keep pace with technology. The march of technology demands the enactment of newer legislation both to regulate the technology and also to facilitate its growth. It was at this point of time that the government of India felt the need to enact the relevant cyber laws which can regulate the Internet in India. Internet and cyberspace need to be regulated and a regulated cyberspace would be the catalyst for the future progress of mankind. Here lay the seeds of origin of cyber law in India.

This research paper is an honest attempt to examine the cyber crimes and their impact on the present legal scenario in India. Part I of this research paper summarizes Actus Reus in cyber crimes, Part II explains mens rea in cyber crimes, Part III investigates classification of various types of cyber crimes, Part IV examines comparative scanning of cases registered and persons arrested under Information Technology Act, Part V deals with changes brought by the Information Technology (Amendment) Act 2008 and Part VI discusses at length suggestions to tackle cyber crimes.

I. ACTUS REUS IN CYBER CRIMES

The element of actus reus in cyber crimes is relatively easy to identify, but it is not always easy to prove. The fact of occurrence of the act that can

be termed as a crime can be said to have taken place when a person is:[1]

(a). trying to make a computer function;

(b). trying to access data stored on a computer or from a computer, which has access to data stored outside.

II. MENS REA IN CYBER CRIMES

There are two vital ingredients for Mens Rea to be applied to a cyber criminal[2]:

(a). The access intended to be secured must have been unauthorized; and

(b). The offender should have been aware of the same at the time he or she tried to secure access.

Mens Rea does not enquire into the mental attitude of the wrong doer but it simply means that the mens rea is judged from the conduct by applying an objective standard. The act is not judged from the mind of the wrong-doer, but the mind of the wrong-doer is judged from the acts. An act which is unlawful can not be excused in law on the ground, that it was committed with a good motive.

To be guilty of cyber crime in India, a person must act voluntarily and willfully. For example, a person who deliberately sends Virii online is guilty of cyber crime but a person who forwards an e-mail without realizing it contains a virus or spreads a virus when his/her account is hacked is not guilty. This means that to constitute a cyber crime in India mens-rea is an essential element along with actus reus. Section 43 (c) read with S/66 amply clears the above point. S/43 mentions penalty and compensation for damage to computer, computer system, etc. whereas S/66 mentions punishment and fine for computer related offences.

III. CLASSIFICATION OF CYBER CRIMES

Cyber crimes are crime related to information technology, electronic commerce etc. Cyber crimes are increasing in all countries and they are bound to explode new legal issues. There are a variety of crimes committed on the Internet but some of them are:

(a). Internet fraud and financial crimes

---

[1] NANDAN KAMATH, LAW RELATING TO COMPUTERS, INTERNET & E-COMMERCE 269 (Universal Law Publishing Co., New Delhi 2000).
[2] *Ibid.*

(b). Online sale of illegal articles

(c). Online gambling

(d). Digital forgery

(e). Cyber defamation

(f). Cyber stalking

(g). Phishing

(h). Cyber terrorism

(i). Cyber conspiracy etc.

These cyber crimes will be discussed one by one. (This list is not exhaustive)

A. Internet Fraud and Financial Crimes

Money is the most common motive behind all crime. The same is also true for cyber crime. More and more cyber crimes are being committed for financial motives rather than for "revenge" or for "fun". There are various fraudulent schemes envisaged over the Internet from which the criminals benefit financially. Various Internet frauds include online auctions, Internet access devices, work-at-home plans, information/adult services, travel/vacations, advance fee loan, prizes etc. Payment method varies from credit/debit card to cheque to even sending cash. Financial crimes include cyber cheating, credit card frauds, money laundering, hacking into bank servers, computer manipulation, accounting scams etc. Internet offers certain unique advantages, which no other medium has, like anonymity and speed. The Internet also offers a global marketplace for consumers and business.[3] These factors together work up to make up a haven for any fraudulent activities online.

The IT Act deals with the crimes relating to Internet fraud and online investment fraud in Sections 43(d), 65 and 66. Under the Indian Penal Code, Internet fraud would be covered by Sections 415 to 420 which relates to cheating.[4]

B. Online Sale of Illegal Articles

Internet is being used now to sell articles which otherwise are not

---

[3] Fraud Section, Criminal Division, U.S. Department of Justice, *available at* http://internetfraud.usdoj.govt.

[4] Statutory provisions are from relevant acts.

permitted to be sold under the law of a country. This would include sale of narcotics, weapons and wildlife, pirated software or music and distribution of data on private persons and organizations etc. by information on websites, auction websites or simply by using email communication. In December 2004, the CEO of Bazee.com was arrested in connection with sale of a CD with objectionable material on the website. The CD was also being sold in the markets in Delhi. The Mumbai City Police and the Delhi Police got into action. The CEO was later released on bail by the Delhi High Court.[5]

Online sale of illegal articles are governed by Section 8 of the Narcotic Drugs and Psychotropic Substances Act, 1985 which prohibits sale or purchase of any narcotic drug or psychotropic substance. Section 7 of the Arms Act, 1959 prohibits sale of any prohibited arms and ammunition, whereas Section 9B of the Indian Explosive Act, 1884 makes sale of any explosive an offence. Wild Life (Protection) Act, 1972 prohibits sale of banned animal products.[6]

C. Online Gambling

Gambling is illegal in many countries. The problem is that virtual casinos are based offshore making them difficult to regulate.[7] That means that people offer gambling services on the Internet from countries where gambling is permitted and players from countries where gambling is illegal play and bet. It is in this situation that the Internet helps the gamblers to evade law.[8]

Section 3 of the Public Gambling Act, 1867 prohibits gambling. Relevant provisions of the IPC dealing with cheating, criminal misappropriation or criminal breach of trust could be applied in cases of online gambling. However, there is no direct law on this point.[9]

D. Digital Forgery

Forgery is creation of a document which one knows is not genuine and yet projects the same as if it is genuine. Digital forgery implies making use of digital technology to forge a document. Desktop publishing systems, color laser and ink-jet printers, color copiers and image scanners enable

---

[5] Suit No. 1279 of 2001, Delhi High Court.
[6] *Supra* note 4.
[7] BBC Online Network, *available at* http://news.bbc.co.uk.
[8] Keith Mench, *Online Gambling*, *available at* http://www.netsafe.org.nz/gambling/gambling-default.asp.
[9] *Supra* note 4.

crooks to make fakes, with relative case of cheques, currency, passports, visas, with certificates, ID cards etc.[10]

Advanced design, copying and publishing technology is enhancing the capability to produce high-quality counterfeit currency and financial instruments such as commercial cheques, traveler's cheques and money-orders. One of the most popular case was that of Abdul Kareem Telgi who along with several others was convicted in India on several counts of counterfeiting stamp papers and postage stamps totaling several billion rupees.[11]

Section 91 of the IT Act amended the provisions of Section 464 of the IPC in relation to "forgery" to include "electronic records" as well.[12]

E. Cyber Defamation

This occurs when defamation takes place with the help of computers or the Internet. In comparison of offline attempt of defamation, online defamation is more vigorous and effective. Quantitatively, the number of people a comment defaming a person might reach is gigantic and hence would effect the reputation of the defamed person much more than would an ordinary publication. Recently cyber defamation came into highlight, when fraud profiles of several high politicians (L.K. Advani[13], Miss Mayawati[14], Dr. Manmohan Singh[15]) appeared on the social networking site "Orkut".

Cyber defamation is covered under Section 499 of IPC read with Section 4 of the IT Act. While Section 499 of IPC provides provision for defamation, Section 4 of IT Act gives legal recognition to electronic records.[16]

F. Cyber Stalking

Cyber stalking is an electronic extension of stalking. Cyber stalking or on-line harassment is a terrifying pursuit of the victim, actions that usually leave no physical cuts or bruises. Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the

---

[10] S.K. VERMA & RAMAN MITTAL, LEGAL DIMENSIONS OF CYBER SPACE 235 (ILI Publications, 2004).
[11] S.C. No-430/2002 (Crime No-545/00).
[12] *Supra* note 4.
[13] Amar Ujala dated August 29, 2007, Regional Daily Newspaper.
[14] Amar Ujala dated August 28, 2007, Regional Daily Newspaper.
[15] Amar Ujala dated August 29, 2007, Regional Daily Newspaper.
[16] *Supra* note 4.

chat-rooms frequented by the victim, constantly bombarding the victim with e-mails etc. Cyber bullying is worse than face-to-face bullying because it has no geographical boundaries. Former Miss India and ad film maker Rani Jeyraj says, "Earlier, if a man wanted to get at you, he would spread rumors. Now the damage can be far worse. It's like having your own newspaper and writing bad things about someone and circulating it worldwide".[17] A recent data confirms the truth:[18]

Cyber Crime Rate	Yes	No	No awareness
Had bad experience in the social networking sites	61.6%	38.4%	-
Received abusive/dirty mails in inboxes from known/unknown sources	78.1%	21.9%	-
Has experienced cyber stalking	37.0%	49.3%	13.7%
Has experienced phishing attacks	50.7%	42.5%	6.8%
Has been impersonated by email account/social networking profiles/websites etc	28.3%	60.3%	11.4%
Has seen his/her "cloned" profile/email ids	41.1%	46.6%	12.3%
Has been a victim of defamatory statements/activities involving him/herself in the cyber space	68.5%	23.3%	8.2%
Has received hate messages in their inboxes/message boards	42.5%	47.9%	9.6%
Has seen his/her morphed pictures	31.5%	57.5%	11.0%
Has been bullied	39.7%	50.7%	9.6%
Has experienced flaming words from others	43.8%	46.6%	9.6%
Victimized by their own virtual friends	45.2%	53.4%	1.4%
Has reported to authorities	37.8%	47.3%	14.9%
Feels women are prone to cyber attacks	74.0%	26.0%	-

Cyber stalking is covered under Section 503 of IPC that is criminal intimation, cyber stalking in effect is criminal intimidation with the help of computers.[19]

G. Phishing

Phishing is a new kind of cybercrime and method of committing online financial fraud. In the cyber world, phishing (also known as carding and spoofing) is a technique that Internet fraudsters lure unsuspecting victims into giving out their personal finance information. It tricks computer users into entering critical and sensitive information in fake websites, which is later used by them for identity theft and swindling user bank accounts. When users respond with the requested information attackers can use it to

[17] Economic Times, Oct. 4, 2007, National Daily Newspaper.
[18] http://www.cybervictims.org.
[19] *Supra* note 4.

gain access to the accounts.[20] The term "phishing" is derived from "fishing" where bait is offered to fish.[21]

The Delhi High Court in the case of NASSCOM v Ajay Sood elaborated upon the concept of "phishing". The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of NASSCOM.[22] The plaintiff had filed the suit inter alia praying for a decree of permanent injunction restraining the defendants from circulating fraudulent e-mails purportedly originating from the plaintiff. The court declared "phishing" on the Internet to be a form of Internet fraud and hence, an illegal act. This case had a unique bend since it was filed not by the one who was cheated but by the organization who was being wrongly represented that is NASSCOM. The court held the act of phishing as passing off and tarnishing the plaintiff's image.

An alternate form of phishing is by installing malicious code on your machine without your knowledge and permission. This code works secretly in the background monitoring all the sites you visit and passwords you type in. It then passes this information to the identity thieves.

Apart from loosing peace of mind, a victim of phishing is robbed of his identity. This means the fraudsters have access to all the bank and credit card information and can make purchases or withdraw cash itself from the victim's account.

The increasing use of electronic channels for payments has posed a new security problem for banks. India's largest bank, the State Bank of India, has reported an attempt at phishing to the Indian Computer Emergency Response Team (CERT-In).[23]

Other banks like HDFC, IDBI, ICICI Bank Home Loans, HSBC, Standard Chartered, ABN Personal Loans, Bank of India and Kotak Mahindra have their phishing sites. The site called www.hadfcbank.com is very much similar to the URL of the actual HDFC Bank's website www.hdfcbank.com. Similarly, the phishing site for IDBI Bank comes with an extra i-www.idbiibank.com.

Sections of IPC and IT Act which are applicable to Internet fraud and online investment fraud covers phishing as well.[24]

---

[20] http://www.us.cert.gov.
[21] Economic Times, June, 2006, National Daily Newspaper.
[22] 119 (2005) DLT 596, 2005 (30) PTC 437 (Del).
[23] http://infotech.indiatimes.com.
[24] *Supra* note 4.

H. Cyber Terrorism

Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computer networks and the information stored therein when done to intimidate or coerce a govt. or its people in the furtherance of political or social objectives.[25]

The F.B.I. has defined cyber terrorism as[26]

> The unlawful use of force or violence against persons or property to intimidate or coerce a govt, the civilian population, or any segment thereof, in furtherance of political or social objectives through the exploitation of systems deployed by the target.

Another definition of Cyber Terrorism is that "It is the premeditated, politically motivated attack against information, computer systems, computer programmes, and the data which result in violence against non-combatant targets by sub-national groups or clandestine agents".[27]

Cyber-terrorism is the use of computers and information technology, particularly the Internet, to cause harm or severe disruption with the aim of advancing the attacker's own political or religious goals as the Internet becomes more pervasive in all areas of human endeavor, individuals or groups can use the anonymity afforded by cyberspace to threaten citizens, specific groups[28] (i.e. members of an ethnic group or belief), communities and entire countries.

From the above definitions, it can easily concluded that "cyber terrorism" refers to two elements:

(i) Cyber Space; and

(ii) Terrorism.

This means that the term necessarily refers to any dangerous, damaging, and destructive activity that takes place in cyber space. There have been reports of Osama Bin Laden and others hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other websites.

Recently F.B.I. has warned America of cyber attacks. It has said that the destruction caused by such cyber attacks can be easily compared to disastrous weapons causing mass destruction of life and property. Internet is used not only for spreading message of Jehad but new techniques of making

---

[25] Nagpal, *Defining Cyber Terrorism*, Asian School of Cyber Laws.
[26] ICFAI Journal of Cyber Law, Vol. 1, No. 1, at 77 (Nov., 2002).
[27] YOGESH BARUA & DENZYI P. DAYAL, 3 CYBER CRIMES (2001).
[28] http://in.wikipedia.org/wiki/cyber-terrorism.

bomb, making new members for terrorist activities, raising funds for terrorist attacks and other heinous motives.[29] Arizona University's "Dark Web Project" claims that on Internet 50 crore pages, 10 lakh pictures, 15 thousand videos, 300 forums related to terrorist activities and more than 30,000 terrorist members exist.

In India alone, 300 websites are hacked every month. The majority of hacked websites are that of govt. organizations, V.I.P.'s and celebrities.[30]

Information Technology Act 2000 completely missed any provision regarding prevention of Cyber terrorism but IT (Amendment) Act, 2008 has severely dealt with cyber terrorism under Section 66/F.[31]

I. Cyber Conspiracy

Nowadays, social networking sites besides trudging long distances to revive with old friends have also become new synonym for criminal conspiracy. Communities set up these networking websites that are though said to be successful tool for social and political discussions but behind this rosy picture is a dark under-belly. In August 2007, Mumbai teenager Adnan Patrawala was kidnapped from the suburbs and later found murdered in Nav Mumbai allegedly by friends he made on Orkut.[32] The 16-year-old boy was lured with a fake female on-line profile "Angel" to a late night meeting in a shopping mall.[33] He was then kidnapped and strangled to death, before his parents could pay the ransom.

Criminal conspiracy is dealt under Sections 120-A and 120-B of Indian Penal Code (IPC). There is no direct provision on this point in IT Act.[34]

IV. COMPARATIVE SCANNING OF CASES REGISTERED & PERSONS ARRESTED UNDER INFORMATION TECHNOLOGY ACT

Cyber crimes may be spiralling but the country is grappling with poor conviction rates in courts. Scanning of data of cases registered and persons arrested under Information Technology Act bears testimony to this fact. The following data[35] shows that controlling cyber crimes needs immediate attention of the authorities at the helm of affairs.

---

[29] Computers & Law, No. 77 (Maneela, May 2010), at 21.
[30] Dainik Jagran, Regional Daily Newspaper (Jan. 23, 2009).
[31] *Supra* note 4.
[32] Times of India, National Daily Newspaper (New Delhi, August 23, 2007).
[33] Economic Times, National Daily Newspaper (Oct. 9, 2007).
[34] *Supra* note 4.
[35] National Crime Records Bureau, Cyber Crimes Statistics 2011.

Table 2 Cyber Crimes/Cases Registered and Person Arrested under Information Technology Act during 2008-2011

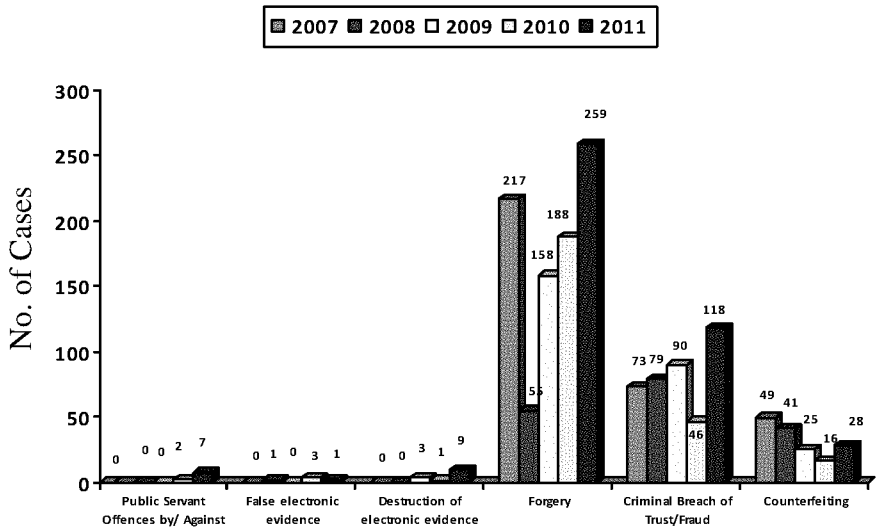
Sl. No.	Crime Heads	Cases Registered				% Variation in 2011 over 2010	Persons Arrested				% Variation in 2011 over 2010
		2008	2009	2010	2011		2008	2009	2010	2011	
1	Tampering computer source documents	26	21	64	94	46.9	26	6	79	66	-16.5
2	Hacking with Computer System i)Loss/Damage to computer resource/utility ii) Hacking	56 82	115 118	346 164	826 157	138.7 -4.3	41 15	63 44	233 61	487 65	109.00 6.6
3	Obscene Publication / transmission in electronic form	105	139	328	496	51.2	90	225	361	443	22.7
4	Failure i) Of compliance/orders of Certifying Authority ii) To assist in decrypting the information intercepted by Govt. Agency	1 0	3 0	2 0	6 3	200 -	1 0	2 0	6 0	4 0	-33.3 @
5	Un-authorised access/attempt to access to protected computer system	3	7	3	5	66.7	0	1	16	15	-6.3
6	Obtaining licence or Digital Signature Certificate by misrepresentation / suppression of fact	0	1	9	6	33.3	11	0	1	0	-100
7	Publishing false Digital Signature Certificate	0	1	2	3	50.0	0	0	0	1	-
8	Fraud Digital Signature Certificate	3	4	3	12	300.0	3	0	6	8	33.3
9	Breach of confidentiality/privacy	8	10	15	26	73.3	3	3	5	27	440.0
10	Other	4	1	30	157	423.3	0	0	0	68	-
	Total	288	420	966	1791	85.4	154	178	288	1184	311.1

Note: @ denotes infinite percentage variation because of division by zero.

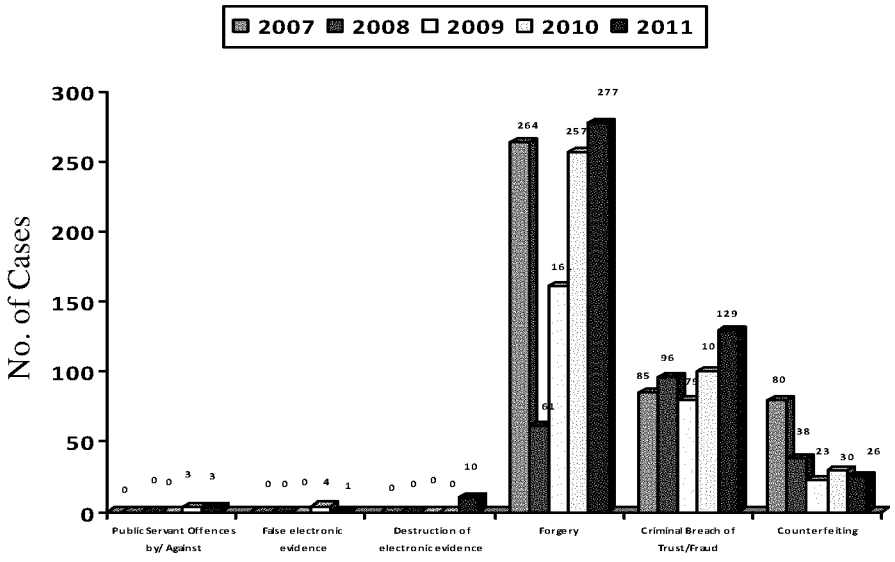
With the legal recognition of electronic records and the amendments made in the several sections of the Indian Penal Code(IPC), 1860 vide the IT Act, 2000 several offences having bearing on cyber-arena are registered under the appropriate sections of the IPC. Besides this law enforcement agencies find easier to handle cybercrime cases under IPC cybercrime cases are not necessarily dealt under the IT Act, 2000. The following graphical

illustration bears testimony to the fact. Offences like Fraud (S/423), Forgery (S/191) and Counterfeiting (S/464) are registered under IPC.

Cyber Crimes/Cases Registered and Persons Arrested under Indian Penal Code during 2007-2011
Cases Registered.



Cyber Crimes/Cases Registered and Persons Arrested under Indian Penal Code during 2007-2011
Persons Arrested.



The National Crime Records Bureau 2011 statistics clearly illustrates that incidence of cyber crimes (IT Act+IPC Sections) has increased by 67.4% in 2011 as compared to 2010 (from 1,322 in 2010 to 2,213 in 2011). Cyber Forgery 61.3% (259 out of total 422) and Cyber Fraud 27.9% (188 out of 422) were the main cases under IPC category for cyber crimes.

V. CHANGES BROUGHT BY THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

The IT Act, 2000 was promulgated twelve years ago primarily to bolster the e-commerce business and not intended to deal with cyber crime issues. When the law was framed, there were no technology like MMS or sophisticated devices like mobile phones, or mobile phones with cameras or Internet connectivity. The IT Act, 2000 was struggling to cope with the change in modern technology. The act remained static while the rest of the world has changed a lot. To justify the need of the hour on December 23rd, 2008 the Parliament of India passed "The Information Technology Amendment Bill 2008".

A. Main Amendments

Compensation limit has been removed from Section 43 (previously it was one crore rupees under IT Act, 2000). Under Section 48 the name of Cyber Regulations Appellate Tribunal has been changed to Cyber Appellate Tribunal. In Section 66, "dishonesty" and "fraudulent" intention has been made necessary.

B. Some New Sections Have Been Introduced to Combat New Offences

S/66A—Punishment for sending offensive messages.

S/66B—Punishment for dishonestly receiving stolen computer resource.

S/66C—Punishment for identity theft.

S/66D—Punishment for cheating by personation by using computer resource.

S/66E—Punishment for violation of privacy.

S/66F—Punishment for cyber terrorism.

S/67A—Punishment for publishing or transmitting of material containing sexually explicit act.

S/67B—Punishment for child pornography.

C. Other Changes

The definition of intermediary has been modified. As the amendments in various sections now intermediaries are made more responsible and liable towards their acts. New Section 67C asks intermediaries to preserve and retain certain records for a stated period. New Section 69B is also quite stringent to intermediaries. Section 69A has been introduced to enable blocking of websites by the central government. Section 69B provides powers to central government to collect traffic data from any computer resource. It could be either in transit or in storage. This amendment was necessary for security purpose but it may lead to abuse of power by government. Section 72A has been introduced to cover offences regarding disclosure of information in breach of lawful contract. Section 80 empowers inspectors instead of D.S.P's to enter, search, etc.

D. Loopholes of Information Technology Act, 2008

ITA-2000 suffer from many loopholes, some of them are removed in ITAA-2008 but some of them prevail even now. The IT Act, 2000 has provided punishment for various cyber offences ranging from three to ten years. These are non-bailable offences where the accused is not entitled to bail as a matter of right.

However, what amazes the lay reader is that the amendments to the IT Act have gone ahead and reduced the quantum of punishment. For example, in Section 67, which relates to offence of online obscenity the quantum of punishment on first conviction for publishing, transmitting or causing to be published any information in the electronic form, which is lascivious and has been reduced from the existing five years to three years. Similarly, the amount of punishment for the offence of failure to comply with the directions of the controller of certifying authorities is reduced from three years to two years. (S/68)

Government has actually relaxed the laws governing some most common cyber offences. Common cyber crimes, such as introducing viruses, cyber stalking, defamation, impersonation and stealing of access codes like passwords and pin numbers are bailable offences under ITAA-2008. Earlier these were non-bailable offences.

Hacking or unauthorized access to a computer system has been deleted from the list of crimes in the ITAA-2008. The original legislation had stipulated jail term up to three years and Rs. 2 lakh fine for hacking, now it has come under the ambit of computer-related offences that are bailable.

The legislation has now stipulated that cyber crimes punishable with

imprisonment of three years shall be bailable offences. Since the majority of cyber crime offences defined under the amended IT Act are punishable with three years, (except-cyber terrorism, child pornography and violation of privacy), the net effect of all amendments is that a majority of these cyber crimes shall be bailable. This means that the moment a cyber criminal will be arrested by the police, barring a few offences, in almost all other cyber crimes, he shall be released on bail as a matter of right by the police, there and then.

It will be but natural to expect that the concerned cyber criminal, once released on bail, will immediately go and evaporate, destroy or delete all electronic traces and trails of his having committed any cyber crime, thus making the job of law enforcement agencies (LEA's) to have cyber crime convictions, near impossibility. This would put the LEA's under extreme pressure.

Section 69 of 2008 Act had given the central government the power to intercept and monitor any information through computer systems in national interest, permitting it to monitor any potentially cognizable offence. This will give government endless power to "intercept or monitor any information through any computer resource". Unauthorized interceptions could soon become common. This is bound to infringe civil liberties like right to privacy or right to anonymous communication with legitimate purposes.

Another major change that ITAA-2008 have done is that cyber crimes in India shall now be investigated not by a Deputy Superintendent of Police, as under ITA-2000 but shall now be done by low level police inspector such an approach is hardly likely to withstand the test of time, given the current non-exposure and lack of training of Inspector level police officers to tackle cyber crimes, their detection, investigation and prosecution.

Having discussed the innumerable negative changes of ITAA-2008, it is also necessary to mention briefly if there are any benefits at all that are envisaged in ITAA-2008.

Certain provisions that have been put in the right frame are as follows: Cyber terrorism and child pornography have been made non-bailable. The law has dealt severely with sections relating to child pornography (S/67B) and cyber terrorism (S/66F). The punishment for child pornography is imprisonment up to 5 years along with a fine up to Rs. 10 Lakhs, while for cyber terrorism, the punishment is imprisonment for life.

Perhaps these provisions can be considered as the silver lining in the otherwise dark cloud.

VI. SUGGESTIONS

Some suggestions to tackle cyber crimes are as follows: There should be clear provisions for handling IPR, domain name issues and related concerns such as cyber squatting certain provisions like electronic payments need urgent and specific attention. Trained officials well trained and equipped police force, investigators with the expert knowledge in computer forensic should be appointed to attain to the grievances of the complainant.

There should be clear briefs on how the act will apply to any offence, and how action will be taken against any person who has committed the crime outside India(S/75). Crimes like cyber theft, cyber stalking, cyber harassment, cyber defamation need to have specific provisions in the act to enable the police to take quick action. To cope with modern cyber crimes (MMS, mobile phones), there is a need for a constant innovation and improvement in the present act. There is a need for incorporating new technologies. There is a further need towards adoption of new technologies.

The IT Act should include special and tighter norms to protect data from theft, frauds, etc. Different provisions concerning privacy need to be appropriately defined specific provisions dealing with problems as spamming need to be incorporated.

Under IT Act, 2000, the authentication technology acceptable was only digital signatures. This is not suffice, so technologies like biometrics which include fingerprints, thumb impression or retina of an eye to prove identity should be recognized. Offences instead of being prosecuted under civil and criminal procedure both, covered under criminal procedure only then the process could be much faster.

To keep a check on cyber terrorism, all cybercafes should be continuously monitored to ensure that they maintain regular and proper records of its users with adequate identity checking procedures being duly adopted as per law, stringent laws should be made regarding cyber terrorism so that terrorists may not use web to commit crimes such as online credit card fraud or using e-mail to plan a crime, a terrorist attack (Taj Hotel Bombay November 26, 2008) or hack into some sites.

If India has to make a quantum jump in law-making, it needs to develop capacities to protect material interests and to avoid exploitation by those who own technology. Government should take note of social networking sites and put in place a proper mechanism to curb the misuse. The IT Act needs to be amended to clarify the rights, obligations and liabilities of bloggers and address blogging as a phenomenon.

The specialized nature of cyber crime requires a specialized response.

It requires cops specially suited and trained to deal with it. Detection of cyber crimes requires Internet research skills, necessary court orders including search warrants of premises and electronic surveillance.

The absolutely poor rate of cyber crime conviction in the country has also not helped the cause of regulating cyber crimes. There have only been few cyber crime convictions in the whole country, which can be counted on fingers. There is a need to ensure specialized procedures associated with expertise manpower for prosecution of cybercrime cases so as to tackle them on a war footing. Investigators and judges should be sensitized to the nuances of the system. It must be ensured that the system provides for stringent punishment of cyber crime and cyber criminals so that the same acts as a deterrent for others. This is necessary so as to win the faith of the people in the ability of the system to tackle cyber crime. Special and fast track courts should be set up to settle cases of cyber crimes expeditiously.

Harmonization of cyber laws across the globe is needed, so that investigating agencies like Central Bureau of investigation (CBI) have more teeth for tackling hi-tech crimes. Although the Department of Information Technology (DIT) has a computer emergency response team (Cert-in) for assisting the combat efforts of law enforcing agencies, it needs to be developed further.

Quick response to the Interpol references and bilateral requests, liberal sharing of forensic technology and more cross-country training exchange programmes besides timely alert could prove a deterrent against the cyber menace. Mobile Hi-tech crime detecting units must be established. Cooperation in investigation from other countries and extradition should be secured for tackling cyber crime.

Internet security does not seem to be a priority with Indian Internet companies. On an average, Indian companies spend less than 1% of their funds on security. This is considerably lower than the worldwide average of 5% and needs to be increased considerably. It requires sincere and effective efforts in this direction.

CONCLUSION

Certainly, revolution was brought about by the introduction of the Internet, but who could think of the time when this rich source of knowledge will be misused for criminal activities. The largest challenge to the law is to keep pace with technology. A combined effort from public, users, technocrats is the dire need of the present time. If the suggestions given above will be followed, cyber crimes will be effectively combated.

Chapter 4

Legal Protection against Cyber Crimes

Cybercrimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet the Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cybercrimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

4.1 Criminal Liabilities under Information Technology Act, 2000

- Sec.65: Tampering with Computer source documents
- Sec.66: Hacking with Computer systems, Data alteration and other computer related Offences
- Sec. 66A: Punishment for sending offensive messages through communication service etc.
- Sec. 66B: Punishment for dishonestly receiving stolen computer resource or communication device
- Sec. 66C: Punishment for identity theft
- Sec. 66D: Punishment for Cheating by personating by using computer resource
- Sec. 66E: Punishment for Violation of Privacy
- Sec. 66F: Punishment for Cyber Terrorism
- Sec.67: Publishing obscene information
- Sec. 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form

- Sec. 67B: Punishment for Child Pornography
- Sec. 67C: Preservation and Retention of Information by Intermediaries
- Sec.70: Un-authorized access to protected system
- Sec. 70A: National Nodal Agency
- Sec. 70B: CERT-in
- Sec. 71: Penalty for Misrepresentation
- Sec.72: Breach of Confidentiality and Privacy
- Sec.73: Publishing false digital signature certificates
- Sec. 74: Publication for fraudulent purposes

The criminal provisions of the IT Act and those dealing with cognizable offences and criminal acts follow from Chapter IX titled "Offences"

Section 65 : *Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.*

Explanation—For the purposes of this section, "computer source code" means the listing of programmes, computer Commands, design and layout and programme analysis of computer resource in any form.

This section deals with Tampering with computer source code and related documents. Concealing, destroying, and altering any computer source code when the same is required to be kept or maintained by law is an offence punishable with three years imprisonment or two lakh rupees or with both. Fabrication of an electronic record or committing forgery by way of interpolations in CD produced as evidence in a court (*Bhim Sen Garg* vs *State of Rajasthan and others*[11])

attract punishment under this Section. Computer source code under this Section refers to the listing of programmes, computer commands, design and layout etc. in any form.

Case Laws

(i) *Frios* vs *State of Kerala*[12]

Facts : In this case it was declared that the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70. The court upheld the validity of both. It included tampering with source code. Computer source code the electronic form, it can be printed on paper.

Held : The court held that tampering with Source code are punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

(ii) *Syed Asifuddin And Ors. vs The State of Andhra Pradesh*[13]

Facts : In this case the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones, theft were exclusively franchised to Reliance Infocom.

Held : Court held that Tampering with source code invokes Section 65 of the Information Technology Act.

(iii) *State vs Mohd. Afzal And Others*[14] *(Parliament Attack Case)*

Facts : In this case several terrorist attacked on 13 December, 2001 Parliament House. In this the Digital evidence played an important role during their prosecution. The accused argued that computers and evidence can easily be tampered and hence should not be relied.

In Parliament case several smart device storage disks and devices, a Laptop were recovered from the truck intercepted at Srinagar pursuant to information given by two suspects. The laptop included the evidence of

fake identity cards, video files containing clips of the political leaders with the background of Parliament in the background shot from T.V. news channels. In this case design of Ministry of Home Affairs car sticker, there was game "wolf pack" with user name of "Ashiq". There was the name in one of the fake identity cards used by the terrorist. No backup was taken therefore it was challenged in the Court.

Held : Challenges to the accuracy of computer evidence should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

Section 66 : *If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.*

Explanation.—For the purpose of this section,—

(a) The word "dishonesty" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860).

(b) The word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

Computer related offences are dealt with under this Section. Data theft stated in Section 43[15] is referred to in this Section. Whereas it was a plain and simple civil offence with the remedy of compensation and damages only, in that Section, here it is the same act but with a criminal intention thus making it a criminal offence. The act of data theft or the offence stated in Section 43 if done dishonestly or fraudulently becomes a punishable offence under this Section and attracts imprisonment upto three years or a fine of five lakh rupees or both. Earlier hacking was defined in Sec 66 and it was an offence.

Now after the amendment, data theft of Section 43 is

being referred to in Section 66 by making this section more purposeful and the word 'hacking' is not used. The word 'hacking' was earlier called a crime in this Section and at the same time, courses on 'ethical hacking' were also taught academically. This led to an anomalous situation of people asking how an illegal activity be taught academically with a word 'ethical' prefixed to it. Then can there be training programmes, for instance, on "Ethical burglary", "Ethical Assault" etc. say for courses on physical defence? This tricky situation was put an end to, by the ITAA when it re-phrased the Section 66 by mapping it with the civil liability of Section 43 and removing the word 'Hacking'. However the act of hacking is still certainly an offence as per this Section, though some experts interpret 'hacking' as generally for good purposes (obviously to facilitate naming of the courses as ethical hacking) and 'cracking' for illegal purposes. It would be relevant to note that the technology involved in both is the same and the act is the same, whereas in 'hacking' the owner's consent is obtained or assumed and the latter act 'cracking' is perceived to be an offence.

Case Laws

1. *R vs. Gold & Schifreen*[16]

   In this case it is observed that the accused gained access to the British telecom Prestly Gold computers networks file amount to dishonest trick and not criminal offence.

2. *R vs. Whiteley*[17]

   In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers. The CBI had registered a cyber crime case against Kumar

and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said.

Verdict: The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).

Thanks to ITAA, Section 66 is now a widened one with a list of offences as follows:

***66A** : Punishment for sending offensive messages through communication service, etc.—Any person who sends, by means of a computer resource or a communication device,— (a) any information that is grossly offensive or has meaning character, or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such message, shall be punishable with imprisonment for a term which may extend to three years and with fine.*

Explanation.—For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created to transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

The section covers the offences like sending offensive messages through communication service, causing annoyance etc. through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing).

Punishment for these acts is imprisonment up to three years or fine.

Case Laws

Fake profile of President posted by imposter

On September 9, 2010, the imposter made a fake profile in the name of the Hon'ble President Smt. Pratibha Devi Singh Patil. A complaint was made from Additional Controller, President Household, President Secretariat regarding the four fake profiles created in the name of Hon'ble President on social networking website, Facebook. The said complaint stated that president house has nothing to do with the facebook and the fake profile is misleading the general public. The First Information Report under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.

Bomb Hoax mail

In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1 p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

66B *Punishment for dishonestly receiving stolen computer resource or communication device.—*

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

The section clearly states that dishonestly receiving stolen computer resource or communication device will be leading to the punishment upto three years or one lakh rupees as fine or both.

66C *Punishment for identity theft -*

Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Electronic signature or other identity theft like using others' password or electronic signature etc.

Punishment is three years imprisonment or fine of one lakh rupees or both.

66D : *Punishment for cheating by personation by using computer resource*

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

In accordance with this section, Cheating by personating using computer resource or a communication device shall be punished with imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Case Laws

Sandeep Vaghese vs. State of Kerala[18]

A complaint filed by the representative of a Company, which was engaged in the business of trading and distribution of petrochemicals in India and overseas, a crime was registered against nine persons, alleging offenses under Sections 65, 66, 66A, C and D of the Information Technology Act along with Sections 419 and 420 of the Indian Penal Code.

The company has a web-site in the name and style `www.jaypolychem.com' but, another web site `www. jayplychem.org' was set up in the internet by first accused Samdeep Varghese @ Sam, (who was dismissed from the company) in conspiracy with other accused, including Preeti and Charanjeet Singh, who are the sister and brother-in-law of `Sam'.

Defamatory and malicious matters about the company and its directors were made available in that website. The accused sister and brother-in-law were based in Cochin and they had been acting in collusion with known and unknown persons, who have collectively cheated the company and committed acts of forgery, impersonation etc.

Two of the accused, Amardeep Singh and Rahul had visited Delhi and Cochin. The first accused and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Bank etc. to malign the name and image of the Company and its Directors. The defamation campaign run by all the said persons named above has caused immense damage to the name and reputation of the Company.

The Company suffered losses of several crores of Rupees from producers, suppliers and customers and were unable to do business.

66E *Punishment for violation of privacy*

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which

may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation.- For the purposes of this section--

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Data Protection and Privacy

This section deals with the punishment for Privacy violation– Publishing or transmitting private area of any person without his or her consent etc. Punishment is three years imprisonment or two lakh rupees fine or both. This section needs to be read along with section 43 and Section 43A which creates civil remedies for data theft wherein section 66 E provides criminal liability for the gross violation of one's privacy.

Cases

(i) *Jawaharlal Nehru University MMS scandal*

In a severe shock to the prestigious and renowned institute – Jawaharlal Nehru University, a pornographic

MMS clip was apparently made in the campus and transmitted outside the university. Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market.

(ii) *Nagpur Congress leader's son MMS scandal*

On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son of a Congress leader, for harassing a 16-year-old girl by circulating an MMS clip of their sexual acts. According to the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, a zila parishad member and an influential Congress leader of Saoner region in Nagpur district.

66F *Punishment For Cyber Terrorism*

(1) Whoever -

(A) With intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

- *denying or cause the denial of access to any person authorized to access computer resource; or*
- *attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or*
- *introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or*

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, 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, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Critique : We find the terminology in multiple sections too vague to ensure consistent and fair enforcement. The concepts of 'annoyance' and 'insult' are subjective. Clause (d) makes it clear that phishing requests are not permitted, but it is not clear that one cannot ask for information on a class of individuals.

Cyber terrorism – Intent to threaten the unity, integrity, security or sovereignty of the nation and denying access to any person authorized to access the computer resource or attempting to penetrate or access a computer resource without authorization. Acts of causing a computer contaminant (like virus or Trojan Horse or other spyware or malware) likely to cause death or injuries to persons or damage to or destruction of property etc. come under this Section. Punishment is life imprisonment.

It may be observed that all acts under Section 66 are cognizable and non-bailable offences. Intention or the

knowledge to cause wrongful loss to others i.e. the existence of criminal intention and the evil mind, i.e., concept of mens rea, destruction, deletion, alteration or diminishing in value or utility of data are all the major ingredients to bring any act under this Section.

To summarise, what was civil liability with entitlement for compensations and damages in Section 43, has been referred to here, if committed with criminal intent, making it a criminal liability attracting imprisonment and fine or both.

Cases

Threat Mail to BSE and NSE[19]

In May 5, 2009, the Mumbai police have registered a case of 'cyber terrorism'—the first in the state since an amendment to the Information Technology Act—where threats email was sent to the BSE and NSE on May 4, 2009. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case. The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab Md with an ID sh.itaiyeb125@yahoo.in to BSE's administrative email ID corp.relations@bseindia.com at around 10.44 am on Monday. The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had, while creating the new ID, given two mobile numbers in the personal details column. Both the numbers belong to a photo frame-maker in Patna," said an officer.

Status : The MRA Marg police have registered forgery for purpose of cheating, criminal intimidation cases under the IPC and a cyber-terrorism case under the IT Act, 2000.

Section 67 *: Publishing of information which is obscene in electronic form*

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to

deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

This section deals with publishing or transmitting obscene material in electronic form. The earlier Section in ITA, 2000 was later widened as per ITAA, 2008 in which child pornography and retention of records by intermediaries were all included.

Publishing or transmitting obscene material in electronic form is dealt with here. Whoever publishes or transmits any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely to read the matter contained in it, shall be punished with first conviction for a term upto three years and fine of five lakh rupees and in second conviction for a term of five years and fine of ten lakh rupees or both.

This Section is of historical importance since the landmark judgement in what is considered to be the first ever conviction under I.T. Act, 2000 in India, was obtained in this Section in the famous case *State of Tamil Nadu* vs.*Suhas Katti*[20] on 5 November, 2004. The strength of the Section and the reliability of electronic evidences were proved by the prosecution and conviction was brought about in this case, involving sending obscene message in the name of a married women amounting to cyber stalking, email spoofing and the criminal activity stated in this Section.

Case Laws

1. *The State of Tamil Nadu vs. Suhas Katti*[21]

   Facts : This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the

victim for information by the accused through a false e-mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the complaint police nabbed the accused. He was a known family friend of the victim and was interested in marrying her. She married to another person, but that marriage ended in divorce and the accused started contacting her once again. And her reluctance to marry him he started harassing her through internet.

Held : The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000 and the accused is convicted and is sentenced for the offence to undergo Rigorous Imprisonment for 2 years under section 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo Rigorous Imprisonment for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.'

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.

In a recent case, a groom's family received numerous emails containing defamatory information about the prospective bride. Fortunately, they did not believe the emails and chose to take the matter to the police. The sender of the emails turned out to be the girl's step-father, who did not want the girl to get married, as he would have lost control over her property, of which he was the legal guardian.

2. *Avnish Bajaj vs. State*[22]

This is famously known as Avnish Bajaj (CEO of bazzee.com – now a part of the eBay group of companies) case.

Facts : There were three accused first is the Delhi school

boy and IIT Kharagpur Ravi Raj and the service provider Avnish Bajaj.

The law on the subject is very clear. The sections slapped on the three accused were Section 292 (sale, distribution, public exhibition, etc., of an obscene object) and Section 294 (obscene acts, songs, etc., in a public place) of the Indian Penal Code (IPC), and Section 67 (publishing information which is obscene in electronic form) of the Information Technology Act, 2000. In addition, the schoolboy faced a charge under Section 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode. These offences invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first time conviction, and/or fines.

Held : In this case the Service provider Avnish Bajaj was later acquitted and the Delhi school boy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days.

3. *Daskhina Kannada police solved the first case of cyber crime in the district*

Dakshina Kannada Police solved a case where a Father at a Christian institution in the city had approached the Superintendent of Police with a complaint that he was getting offensive and obscene e-mails.

Police said that all the three admitted that they had done this to tarnish the image of the Father. As the three tendered an unconditional apology to the Father and gave a written undertaking that they would not repeat such act in future, the complainant withdrew his complaint. Following this, the police dropped the charges against the culprit.

The release said that sending of offensive and obscene e-mails is an offence under the Indian Information Technology Act 2000.

Section 67-A *Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form:*

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

- *the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or*
- *which is kept or used bona fide for religious purposes.*

It deals with publishing or transmitting of material containing sexually explicit act in electronic form. Contents of Section 67 when combined with the material containing sexually explicit material attract penalty under this Section.

Section 67B *: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form:*

Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or

distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) Facilitates abusing children online or

(e) Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Child Pornography has been exclusively dealt with under Section 67B. Depicting children engaged in sexually explicit act, creating text or digital images or advertising or promoting such material depicting children in obscene or indecent manner etc or facilitating abusing children online

or inducing children to online relationship with one or more children etc come under this Section.

'Children' means persons who have not completed 18 years of age, for the purpose of this Section. Punishment for the first conviction is imprisonment for a maximum of five years and fine of ten lakh rupees and in the event of subsequent conviction with imprisonment of seven years and fine of ten lakh rupees.

Bonafide heritage material being printed or distributed for the purpose of education or literature etc. are specifically excluded from the coverage of this Section, to ensure that printing and distribution of ancient epics or heritage material or pure academic books on education and medicine are not unduly affected.

Screening video graphs and photographs of illegal activities through Internet all come under this category, making pornographic video or MMS clippings or distributing such clippings through mobile or other forms of communication through the Internet fall under this category.

Section 67C fixes the responsibility to intermediaries that they shall preserve and retain such information as may be specified for such duration and in such manner as the Central Government may prescribe. Non-compliance is an offence with imprisonment up to three years or fine.

` **Case Laws**

Janhit Manch & Ors. vs. The Union of India[23]

In this case it was Public Interest Litigation to ban child pornography. The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

Transmission of electronic message and communication:

Section 69: Powers to issue directions for interception or

monitoring or decryption of any information through any computer resource:

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

[Section 69B] Power to authorize to monitor and collect

traffic data or information through any computer resource for Cyber Security:

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection

(2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Critique: Though we recognize how important it is for a government to protect its citizens against cyber-terrorism, we are concerned at the friction between these provisions

and the guarantees of free dialog, debate, and free speech that are Fundamental Rights under the Constitution of India.

Specifically:

(a) There is no clear provision of a link between an intermediary and the information or resource that is to be monitored.

(b) The penalties laid out in the clause are believed to be too harsh, and when read in conjunction with provision 66, there is no distinction between minor offenses and serious offenses.

(c) The ITA is too broad in its categorization of acts of cyber terrorism by including information that is likely to cause: injury to decency, injury to morality, injury in relation to contempt of court, and injury in relation to defamation.

This is an interesting section in the sense that it empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance of procedure as laid down here.

This power can be exercised if the Central Government or the State Government, as the case may be, is satisfied that it is necessary or expedient in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence. In any such case too, the necessary procedure as may be prescribed, is to be followed and the reasons for taking such action are to be recorded in writing, by order, directing any agency of the appropriate Government. The subscriber or intermediary shall extend all facilities and technical assistance when called upon to do so.

Cases

Posting Insulting Images of Chhatrapati Shivaji:

In August 2007, Lakshmana Kailash K., a techie from

Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut. The police identified him based on IP address details obtained from Google and Airtel -Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 p.m.

Verdict : Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages. The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights.

Section 69A *: Power to issue directions for blocking for public access of any information through any computer resource*

(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction

issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

The section as inserted in the ITAA, vests with the Central Government or any of its officers with the powers to issue directions for blocking for public access of any information through any computer resource, under the same circumstances as mentioned above.

Section 69B discusses the power to authorise to monitor and collect traffic data or information through any computer resource.

Commentary on the powers to intercept, monitor and block websites

In short, under the conditions laid down in the Section, power to intercept, monitor or decrypt does exist. It would be interesting to trace the history of telephone tapping in India and the legislative provisions (or the lack of it) in our nation and compare it with the powers mentioned here. Until the passage of this Section in the ITAA, phone tapping was governed by Clause 5(2) of the Indian Telegraph Act of 1885, which said that "On the occurrence of any public emergency, or in the interest of the public safety, the Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order". Other sections of the act mention that the government should formulate "precautions to be taken for preventing the improper interception or disclosure of messages". There have been many attempts, rather many requests, to formulate rules to

govern the operation of Clause 5(2). But ever since 1885, no government has formulated any such precautions, maybe for obvious reasons to retain the spying powers for almost a century.

A writ petition was filed in the Supreme Court in 1991 by the People's Union for Civil Liberties, challenging the constitutional validity of this Clause 5(2). The petition argued that it infringed the constitutional right to freedom of speech and expression and to life and personal liberty.

In December 1996, the Supreme Court delivered its judgment, pointing out that "unless a public emergency has occurred or the interest of public safety demands, the authorities have no jurisdiction to exercise the powers" given to them under Clause 5(2). They went on to define them thus: a public emergency was the "prevailing of a sudden condition or state of affairs affecting the people at large calling for immediate action", and public safety "means the state or condition of freedom from danger or risk for the people at large". Without those two, however "necessary or expedient", it could not do so. Procedures for keeping such records and the layer of authorities etc were also stipulated.

Now, this **Section 69 of ITAA is far more intrusive** and more powerful than the above-cited provision of Indian Telegraph Act 1885. Under this ITAA Section, the nominated Government official will be able to listen in to all phone calls, read the SMSs and emails, and monitor the websites that one visited, subject to adherence to the prescribed procedures and without a warrant from a magistrate's order. In view of the foregoing, this Section was criticised to be draconian vesting the government with much more powers than required.

Having said this, we should not be oblivious to the fact that this power (of intercepting, monitoring and blocking) is something which the Government represented by the **Indian Computer Emergency Response Team**, (the National Nodal Agency, as nominated in Section 70B of ITAA) has very rarely exercised. Perhaps believing in the freedom

of expression and having confidence in the self-regulative nature of the industry, the CERT-In has stated that these powers are very sparingly (and almost never) used by it.

Critical Information Infrastructure and Protected System have been discussed in Section 70.

The Indian Computer Emergency Response Team (CERT-In) coming under the Ministry of

Information and Technology, Government of India, has been designated as the National Nodal Agency for incident response. By virtue of this, CERT-In will perform activities like collection, analysis and dissemination of information on cyber incidents, forecasts and alerts of cyber security incidents, emergency measures for handling cyber security incidents etc.

The role of CERT-In in e-publishing security vulnerabilities and security alerts is remarkable.

The then Minister of State for Communications and IT Mr.Sachin Pilot said in a written reply to the Rajya Sabha said that (as reported in the Press), CERT-In has handled over 13,000 such incidents in 2011 compared to 8,266 incidents in 2009. CERT-In has observed that there is significant increase in the number of cyber security incidents in the country. A total of 8,266, 10,315 and 13,301 security incidents were reported to and handled by CERT-In during 2009, 2010 and 2011, respectively, "

These security incidents include website intrusions, phishing, network probing, spread of malicious code like virus, worms and spam, he added. Hence the role of CERT-In is very crucial and there are much expectations from CERT In not just in giving out the alerts but in combating cyber crime, use the weapon of monitoring the web-traffic, intercepting and blocking the site, whenever so required and with due process of law.

Penalty for breach of confidentiality and privacy is discussed in Section 72 with the punishment being imprisonment for a term upto two years or a fine of one lakh rupees or both.

***Section 71**: Penalty for misrepresentation*

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Penalties:

Punishment : imprisonment which may extend to two years

Fine : may extend to one lakh rupees or with both.

***Section 72** : Penalty for breach of confidentiality and privacy*

Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: This section relates to any to any person who in pursuance of any of the powers conferred by the Act or it allied rules and regulations has secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

If such person discloses such information, he will be punished with punished. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

Penalties :

Punishment : term which may extend to two years.

Fine: one lakh rupees or with both.

Section 72A *: Punishment for Disclosure of information in breach of lawful contract*

Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Section 73 *: Penalty for publishing electronic Signature Certificate false in certain particulars:*

No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

- *the Certifying Authority listed in the certificate has not issued it; or*
- *the subscriber listed in the certificate has not accepted it; or*
- *the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation*

Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation : The Certifying Authority listed in the certificate has not issued it or,

The subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

The Certifying authority may also suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offence it is the purpose of verifying a digital signature created prior to such suspension or revocation.

Penalties:

Punishment: imprisonment of a term of which may extend to two years.

Fine: fine may extend to 1 lakh rupees or with both

Case Laws

Bennett Coleman & Co. v/s Union of India[24]

In this case the publication has been stated that ?publication means dissemination and circulation. In the context of digital medium, the term publication includes and transmission of information or data in electronic form.

Section 74 – *Publication for fraudulent purpose:*

Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 75 *– Act to apply for offence or contraventions committed outside India*

Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

4.2 Common Cyber Crimes and Applicable Legal Provisions : A Snapshot

S.No.	*Cyber Crime*	*Applicable Provisions*
1.	*Harassment via fake public profile on social networking site* :A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labeled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim	*Sections 66A, 67 of IT* Act and Section 509 of the Indian Penal Code.
2.	*Online Hate Community* : Online hate community is created inciting a religious group to act orpass objectionable remarks against a country, national figures etc.	Section 66A of IT Act and 153A & 153B of the Indian Penal Code.
3.	*Email Account Hacking :* If victim's email account is hacked and obscene emails are sent to people in victim's address book	Sections 43, 66, 66A, 66C, 67, 67A and 67B of Information Technology Act.
4.	*Credit Card Fraud* : Unsuspecting victims would use infected computers to make online transactions.	Sections 43, 66, 66C, 66D of IT Act and section 420 of the Indian Penal Code.
5.	*Web Defacement* : The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days	Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.
6.	*Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs* : All of the above are some sort of	Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.

S.No.	Cyber Crime	Applicable Provisions
	malicious programs which are used to destroy or gain access to some electronic information	
7.	*Cyber Terrorism* : Many terrorists are use virtual (G-Drive, FTP sites) and physical stoarage media (USB's) hard drives) for hiding information and records of their illicit business.	Conventional terrorism laws may apply along with Section 69 of IT Act.
8.	*Online sale of illegal Articles :* Where sale of narcotics, drugs weapons and wildlife is facilitated by the Internet	Generally conventional laws apply in these cases.
9.	*Cyber P ornography :* Among the largest businesses on Internet. Pornography may not be illegal in many countries, but child pornography is prohibited at large.	Sections 67, 67A and 67B of the IT Act.
10.	*Phishing and Email Scams :* Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity. (E.g. Passwords, credit card information)	Section 66, 66A and 66D of IT Act and Section 420 of IPC
11.	*Theft of Confidential Information* : Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.	Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.
12.	*Source Code Theft* : A Source code generally is the most coveted and important "crown jewel" asset of a company.	Sections 43, 66, 66B of IT Act and Section 63 of Copyright Act.

S.No.	*Cyber Crime*	*Applicable Provisions*
13.	*Tax Evasion and Money Laundering :* Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities.	Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.
14.	*Online Share Trading Fraud :* It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.	Sections 43, 66, 66C, 66D of IT Act and Section 420 of Indian Penal Code.

4.3 Civil Liabilities under Information Technology Act, 2000

The concept of accrued liability applies only to substantive laws and not to procedural laws as no one can claim a vested right in the procedure. In India we have both substantive and procedural laws. The Indian Penal Code and Information Technology Act are substantive laws whereas the Indian Evidence Act, Criminal Procedure Code and Civil procedure Code are procedural laws. Thus, by a retrospective law the procedure can be amended, changed or even repealed. Similarly, the protection of Article 20(1) is available for and can be seeked against criminal matters only and it does not extend to civil matters'. Thus, a civil liability can be enhanced with retrospective effect.

Data Protection

According to the Section: 43-whoever destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine up to 1crore to the person so affected by way of remedy.

Section 43A *which is inserted by 'Information Technology (Amendment) Act, 2008 states that where a body corporate*

is maintaining and protecting the data of the persons as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected. And Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both.

Section 43A of IT Act deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term 'sensitive personal data,' nor has it prescribed a standard and reasonable security practice. Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law. However, Explanation (ii) to Section 43A is worded in such a way that there is lack of clarity whether it would be possible for banks, (or anybody corporate) to enter into agreement which stipulate standards lesser than those prescribed by Central Government and in the event of the contradiction (between the standards prescribed by the Central Government and those in the agreement) which would prevail. Whether a negligence or mala fide on the part of the customer would make the financial institution liable for no fault of it or whether by affording too much protection to banks, a customer is made to suffer are the two extremes of the situation. The need is for striking a balance between consumer protection and protection of the banks from liability due to no fault of theirs. Apart from affording protection to personal data (sensitive personal data- 43A), the IT Act, 2000 also prescribes civil and criminal liabilities (Section 43 and Section 66 respectively) to any person who without the permission of the owner or any other person who is in charge of a computer, computer system etc., inter alia, downloads, copies or extracts any data or damages or causes to be damaged any computer data base etc. In this context Section 72 and 72A of the amended IT Act, 2000 are also of relevance. Section 72 of the Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act, 2000, has secured access to any

electronic record, information etc. and without the consent of the person concerned discloses such information to any other person then he shall be punished with imprisonment up to two years or with fine up to one lakh or with both. Section 72A on the other hand provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract. The purview of Section 72A is wider than section 72 and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of powers granted under IT Act, 2000.

Critical Analysis: Comparative Jurisdiction

However, the attempt is such a limited one, and so replete with shortcomings that the need for a proper data protection law still stands. Given the proposed initiation of the UID scheme, in particular, there is a compelling need for a robust and intelligent law in this regard. Most other countries regimes clearly do at least the following:

- Define and classify types of data (for example, in most European countries, personal data is any data that identifies an individual, sensitive personal data is data that reveals details of ethnicity, religion, health, sexuality, political opinion, etc.),
- Fine-tune the nature of protection to the categories of data (i.e., greater standards of care around sensitive personal data),
- Apply equally to data stored offline and manually as to data stored on computer systems,
- Distinguish between a data controller (i.e., one who takes decisions as to data) and a data processor (i.e., one who processes data on the instructions of the data controller),
- Impose clear restrictions on the manner of data collection (for example, must be obtained fairly and lawfully),
- Give clear guidelines on the purposes for which that data can be put to and by whom (often involving a consent requirement that gives the individual a great degree of control over their data),

- Require certain standards and technical measures around the collection, storage, access to, protection, retention and destruction of data,
- Ensure that the use of data is adequate, relevant and not excessive given the purpose for which it was gathered,
- Cater for opt-in and opt-out type regimes, again to provide individuals with a measure of control over the use of their data even after the stage of initial collection (which has a huge impact on invasive telemarketing or unsolicited written communication),
- Impose a knowledge requirement and procedures for allowing individuals to seek information on what data is held on them, and
- Create safeguards and penalties that are well tailored to breaches of any of the above.

Unfortunately, and perhaps understandably, the ITA barely begins to scratch the surface of what a good data protection regime entails. The provisions that it does introduce (sections 43-A and 72-A) have glaring inadequacies which are as follows:

- The term sensitive personal data or information is used indiscriminately without any definition,
- The provisions only cover electronic data and records, not data stored in non-electronic systems or media,
- They offer no guidance on most of the principles set out above such as in relation to accuracy, adequacy, consent, purpose, etc.,
- In the absence of the controller-processor distinction, liability is imposed on persons, who are not necessarily in a position to control data, even if it is in their possession,
- Civil liability for data breaches only arises where negligence is involved (i.e., failure to have security procedures or failure to implement them correctly will not automatically result in damages unless negligence is proven),

- Similarly, criminal liability only applies to cases of information obtained in the context of a service contract, and requires an element of willfulness, or a disclosure without consent or in breach of a lawful contract – this is a very limited remit aimed largely at preventing disgruntled or unscrupulous employees from dealing in company/customer data.

In addition to the criticisms levelled at the data protection provisions, the other large subset of concerns has been in relation to the civil liberties implications of the ITA. There has been some horror expressed in various forums and media about the ITA contributing to the growth of a police state, to severe curtailment of the freedom of speech and expression, to the invasion of privacy, and to the disproportionate severity of penalization for offences that are placed on crimes committed in cyberspace compared to crimes committed in the here and now. Sadly, this is true to a large extent given the clunky treatment of cyber terrorism, the intolerable pre-censorship that is enabled by the blocking of websites, the broad approach to the monitoring and collection of data, and the demanding obligations of intermediaries to cooperate with interception, monitoring and decryption of data for poorly defined reasons.

While our Constitution's fundamental rights chapter, which enshrines certain basic, democratic, and profound rights, might not have the same vocabulary of due process as we see in the US, it nevertheless requires restrictions to be reasonable. Precedents and the wider jurisprudence in the field have further developed the concepts of checks and balances, procedural safeguards and legitimacy of restraints that a functioning democracy like India must accord to its people. It can be argued that several provisions of the ITA cause significant tension with the right to freedom of speech and expression, the right against self-incrimination, the right to equality before the law, and the right to practice a trade or profession.

Privacy and surveillance

This topic pulls together concerns around the blanket

monitoring and collecting of traffic data or information, the interception and decryption (under duress) by intermediaries (now a large superset of ISPs, search engines, cyber cafes, online auction sites, online market places, etc.) and the wide definition of cyber terrorism (which ludicrously even casts defamation as a terrorist activity).

Some of the broad concerns in relation to interception, monitoring and decryption in (section 69) are that:

- There is no provision for a clear nexus between an intermediary and the information or resource sought to be monitored or intercepted,
- The usual internationally recognised exception to liability where an intermediary operates purely as a conduit and has no control over data flowing through its network is not clearly spelt out,
- The penalties for non-cooperation are extremely harsh, especially given the absence of a) and b) above,
- These onerous penalties can be said to be in violation of Article 14 as they seem entirely disproportionate. Similar offences and remedies in the Code of Criminal Procedure or the Indian Penal Code prescribe less severe penalties, by an order of magnitude in fact. When the only difference between the offences is the medium in which information is contained, it seems arbitrary to impose a much harsher punishment on an online intermediary than on a member of the public who, for example, furnishes false information to the police in connection with a trial or enquiry,
- The rules made in relation to monitoring, interception and decryption, offer some procedural safeguards, in that they impose a time limit on how long a directive for interception or monitoring can remain in force, a ceiling on how long data can be kept before it is required to be destroyed, etc. However, the effect of these is greatly diluted by exceptions for functional requirements, etc. The astonishing irony is that rule 20 requires the intermediary to maintain 'extreme secrecy', 'utmost care

and precaution' in the matter of interception, monitoring or decryption of information as it affects the privacy of citizens.

In a similar vein, there are concerns around the monitoring and collection of traffic data (Section 69B) as the section contains an unreasonably long list of grounds for monitoring. These include such extreme excesses as forecasting of imminent cyber incidents, monitoring network application with traffic data or information on computer resource, identification and determination of viruses/ computer contaminant, and the catch-all any other matter relating to cyber security.

Finally, the main criticism of the ITA approach to cyber terrorism is the very wide net that it seeks to cast, looking for a game that has little or nothing to do with the named offence. Amongst the cast of creatures unwittingly caught during this fishing expedition, we find some unlikely victims. In addition to the usual grounds of offence against sovereignty, national security, defence of India, etc., which we have seen in relation to other sections, the ITA considers the following as acts of cyber terrorism broadly speaking, unauthorized access to information that is likely to cause:

- Injury to decency,
- Injury to morality,
- Injury in relation to contempt of court, and
- Injury in relation to defamation.

This would almost be laughable if these grounds were not enacted into law, posing a threat to civil liberties by their very existence. Other countries have some notion of political ideology, religious case, etc. in their view of terrorism. Indian Law on Information and Communication Technology has been shoehorned into a clause that imposes the stiffest penalty within the entire ITA (life imprisonment) gives even more cause for concern.

4.4 Civil Liability for Corporate:

As mentioned above, anybody corporate who fails to

observe data protection norms may be liable to pay compensation if:

- It is negligent in implementing and maintaining reasonable security practices, and thereby
- Causes wrongful loss or wrongful gain to any person;

Claims for compensation are to be made to the adjudicating officer appointed under section 46 of the IT Act.

4.5 Cyber Crimes under IPC and Special Laws

4.5.1 The Indian Penal Code, 1860

Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many a times since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well.

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc. (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc.) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC under section 463, 464, 468 and 469 read with the ITA/ITAA under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

4.5.2 Cyber Crimes under the Special Acts

- Online sale of Drugs - Narcotic Drugs and Psychotropic Substances Act, 1985.
- Online sale of Arms – Arms Act, 1959.

***

Sharat Babu Digumarti v State Govt. of (NCT of Delhi)

2016 Indlaw SC 892

Bench: Dipak Misra, Prafulla C. Pant, JJ.

The Judgment was delivered by: Dipak Misra, J.

2. The appellant along one Avnish Bajaj and others was arrayed as an accused in FIR No. 645 of 2004. After the investigation was concluded, charge sheet was filed before the learned Metropolitan Magistrate who on 14.02.2006 took cognizance of the offences punishable under Sections 292 and 294 of the Indian Penal Code (IPC) and Section 67 of the Information Technology Act, 2000 ("the IT Act") against all of them. Avnish Bajaj filed Criminal Misc. Case No. 3066 of 2006 for quashment of the proceedings on many a ground before the High Court of Delhi which vide order dated 29.05.2008 came to the conclusion that prima facie case was made out under Section 292 IPC, but it expressed the opinion that Avinish Bajaj, the petitioner in the said case, was not liable to be proceeded under Section 292 IPC and, accordingly, he was discharged of the offence under Sections 292 and 294 IPC. However, he was prima facie found to have committed offence under Section 67 read with Section 85 of the IT Act and the trial court was directed to proceed to the next stage of passing of order of charge uninfluenced by the observations made in the order of the High Court.

3. Being grieved by the aforesaid order, Avnish Bajaj preferred Criminal Appeal No. 1483 of 2009. The said appeal was tagged with Ebay India Pvt. Ltd. v. State and Anr. 2012 Indlaw SC 508 (Criminal Appeal No. 1484 of 2009). The said appeals were heard along with other appeals that arose from the lis relating to interpretation of Sections 138 and 141 of the Negotiable Instruments Act, 1881 (for short, "NI Act") by a three-Judge Bench as there was difference of opinion between the two learned Judges in Aneeta Hada v. Godfather Travels and Tours (P) Ltd. (2008) 13 SCC 703 2008 Indlaw SC 1015.

4. Regard being had to the pleas raised by Avnish Bajaj and also the similarity of issue that arose in the context of NI Act, the three-Judge Bench stated the controversy that emerged for consideration thus:-

"2. In Criminal Appeals Nos. 1483 and 1484 of 2009, the issue involved pertains to the interpretation of Section 85 of the Information Technology Act, 2000 *(for short "*the 2000 Act*") which is in pari materia with Section 141 of the Act. Be it noted, a Director of the appellant Company was prosecuted under Section 292 of the* Penal Code, 1860 *and Section 67 of* the 2000 Act *without impleading the Company as an accused. The initiation of prosecution was challenged under Section 482 of the* Code of Criminal Procedure *before the High Court and the High Court held that offences are made out against the appellant Company along with the Directors under Section 67 read with Section 85 of* the 2000 Act *and, on the said base, declined to quash the proceeding.*

3. The core issue that has emerged in these two appeals is whether the Company could have been made liable for prosecution without being impleaded as an accused and whether the Directors could have been prosecuted for offences punishable under the aforesaid provisions without the Company being arrayed as an accused."

6. As far as the appeal of Avnish Bajaj is concerned, the Court referred to Section 85 of the IT Act which is as follows:-

7. Interpreting the same, the Court opined thus:-

"64. Keeping in view the anatomy of the aforesaid provision, our analysis pertaining to Section 141 of the Act would squarely apply to the 2000 enactment. Thus adjudged, the Director could not have been held liable for the offence under Section 85 of the 2000 Act. *Resultantly, Criminal Appeal No. 1483 of 2009 is allowed and the proceeding against the appellant is quashed. As far as the Company is concerned, it was not arraigned as an accused. Ergo, the proceeding as initiated in the existing incarnation is not maintainable either against the company or against the Director. As a logical sequitur, the appeals are allowed and the proceedings initiated against Avnish Bajaj as well as the Company in the present form are quashed."*

8. After the judgment was delivered, the present appellant filed an application before the trial court to drop the proceedings against him. The trial court partly allowed the application and dropped the proceedings against the appellant for offences under Section 294 IPC and Section 67 of the IT Act,

however, proceedings under Section 292 IPC were not dropped, and vide order 22.12.2014, the trial court framed the charge under Section 292 IPC.

9. Being aggrieved by the order framing of charge, the appellant moved the High Court in Criminal Revision No. 127 of 2015 and the learned Single Judge by the impugned order declined to interfere on the ground that there is sufficient material showing appellant's involvement to proceed against him for the commission of the offence punishable under Section 292 IPC. It has referred to the allegations made against him and the responsibility of the appellant and thereafter referred to the pronouncements in P. Vijayan v. State of Kerala and Anr., (2010) 2 SCC 398 2010 Indlaw SC 58 and Amit Kapoor v. Ramesh Chander and Anr., (2012) 9 SCC 460 2012 Indlaw SC 309 which pertain to exercise of revisional power of the High Court while dealing with propriety of framing of charge under Section 228 of the Code of Criminal Procedure.

10. The central issue that arises for consideration is whether the appellant who has been discharged under Section 67 of the IT Act could be proceeded under Section 292 IPC.

17. At the outset, we may clarify that though learned counsel for the appellant has commended us to certain authorities with regard to role of the appellant, the concept of possession and how the possession is not covered under Section 292 IPC, we are not disposed to enter into the said arenas. We shall only restrict to the interpretative aspect as already stated. To appreciate the said facet, it is essential to understand certain provisions that find place in the IT Act and how the Court has understood the same. That apart, it is really to be seen whether an activity emanating from electronic form which may be obscene would be punishable under Section 292 IPC or Section 67 of the IT Act or both or any other provision of the IT Act.

18. On a perusal of material on record, it is beyond dispute that the alleged possession of material constitutes the electronic record as defined under Section 2(1)(t) of the IT Act. The dictionary clause reads as follows:

"Section 2(1)(t). electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;"

Thus, the offence in question relates to electronic record.

22. In Devidas Ramachandra Tuljapurkar v. State of Maharashtra and Ors, (2015) 6 SCC 1 two-Judge Bench has opined that as far as test of obscenity is concerned, the prevalent test is the contemporary community standards test. It is apt to note here that in the said case the Court was dealing with the issue, what kind of test is to be applied when personalities like Mahatma Gandhi are alluded. The Court held:-

"142. When the name of Mahatma Gandhi is alluded or used as a symbol, speaking or using obscene words, the concept of "degree" comes in. To elaborate, the "contemporary community standards test" becomes applicable with more vigour, in a greater degree and in an accentuated manner. What can otherwise pass of the contemporary community standards test for use of the same language, it would not be so, if the name of Mahatma Gandhi is used as a symbol or allusion or surrealistic voice to put words or to show him doing such acts which are obscene. While so concluding, we leave it to the poet to put his defence at the trial explaining the manner in which he has used the words and in what context. We only opine that view of the High Court pertaining to the framing of charge under Section 292 IPC *cannot be flawed."*

23. Reference to Shreya Singhal 2015 Indlaw SC 211 (supra) is only to show that in the said case the Court while dealing with constitutional validity of Section 66-A of the IT Act noticed that the said provision conspicuously did not have the word "obscene". It did not say anything else in that regard. In the case at hand, it is required to be seen in which of the provision or both an accused is required to be tried. We have already reproduced Section 292 IPC in the present incarnation. Section 67 of the IT Act which provides for punishment for publishing or transmitting obscene material in electronic form reads as follows:-

25. Section 69 of the IT Act provides for power to issue directions for interception or monitoring or decryption of any information through any computer resource. It also carries a penal facet inasmuch as it states that the subscriber or intermediary who fails to comply with the directions issued under sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be

liable to fine.

26. We have referred to all these provisions of the IT Act only to lay stress that the legislature has deliberately used the words "electronic form". Dr. Singhvi has brought to our notice Section 79 of the IT Act that occurs in Chapter XII dealing with intermediaries not to be liable in certain cases. Learned counsel has also relied on Shreya Singhal 2015 Indlaw SC 211 (supra) as to how the Court has dealt with the challenge to Section 79 of the IT Act. The Court has associated the said provision with exemption and Section 69A and in that context, expressed that:-

"121. It must first be appreciated that Section 79 is an exemption provision. Being an exemption provision, it is closely related to provisions which provide for offences including Section 69-A. We have seen how under Section 69-A blocking can take place only by a reasoned order after complying with several procedural safeguards including a hearing to the originator and intermediary. We have also seen how there are only two ways in which a blocking order can be passed-one by the Designated Officer after complying with the 2009 Rules and the other by the Designated Officer when he has to follow an order passed by a competent court. The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69-A read with the 2009 Rules.

122. Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook, etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject-matters laid down in Article 19(2). Unlawful acts beyond what is laid down in Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).

123. The learned Additional Solicitor General informed us that it is a common practice worldwide for intermediaries to have user agreements containing what is stated in Rule 3(2). However, Rule 3(4) needs to be read down in the same manner as Section 79(3)(b). The knowledge spoken of in the said sub-rule must only be through the medium of a court order. Subject to this, the Information Technology (Intermediaries Guidelines) Rules, 2011 *are valid."*

27. We have referred to the aforesaid aspect as it has been argued by Dr. Singhvi that the appellant is protected under the said provision, even if the entire allegations are accepted. According to him, once the factum of electronic record is admitted, Section 79 of the IT Act must apply ipso facto and ipso jure. Learned senior counsel has urged Section 79, as the language would suggest and keeping in view the paradigm of internet world where service providers of platforms do not control and indeed cannot control the acts/omissions of primary, secondary and tertiary users of such internet platforms, protects the intermediary till he has the actual knowledge. He would contend that Act has created a separate and distinct category called 'originator' in terms of Section 2(1) (z)(a) under the IT Act to which the protection under Section 79 of the IT Act has been consciously not extended. Relying on the decision in Shreya Singhal 2015 Indlaw SC 211 (supra), he has urged that the horizon has been expanded and the effect of Section 79 of the IT Act provides protection to the individual since the provision has been read down emphasizing on the conception of actual knowledge. Relying on the said provision, it is further canvassed by him that Section 79 of the IT Act gets automatically attracted to electronic forms of publication and transmission by intermediaries, since it explicitly uses the non-obstante clauses and has an overriding effect on any other law in force. Thus, the emphasis is on the three provisions, namely, Sections 67, 79 and 81, and the three provisions, according to Dr. Singhvi, constitute a holistic trinity.

28. Having noted the provisions, it has to be recapitulated that Section 67 clearly stipulates punishment for publishing, transmitting obscene materials in electronic form. The said provision read with Section 67A and 67B is a complete code relating to the offences that are covered under the IT Act. Section 79, as has been interpreted, is an exemption provision conferring protection to the individuals. However, the said protection has been expanded in the dictum of Shreya Singhal 2015 Indlaw SC 211 (supra) and we concur with the same. Section 81 also specifically provides that the provisions of the Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. All provisions will have their play and significance, if the alleged offence pertains to offence of electronic

record. It has to be borne in mind that IT Act is a special enactment. It has special provisions. Section 292 of the IPC makes offence sale of obscene books, etc. but once the offence has a nexus or connection with the electronic record the protection and effect of Section 79 cannot be ignored and negated. We are inclined to think so as it is a special provision for a specific purpose and the Act has to be given effect to so as to make the protection effective and true to the legislative intent. This is the mandate behind Section 81 of the IT Act. The additional protection granted by the IT Act would apply.

32. If legislative intendment is discernible that a latter enactment shall prevail, the same is to be interpreted in accord with the said intention. We have already referred to the scheme of the IT Act and how obscenity pertaining to electronic record falls under the scheme of the Act. We have also referred to Sections 79 and 81 of the IT Act. Once the special provisions having the overriding effect do cover a criminal act and the offender, he gets out of the net of the IPC and in this case, Section 292. It is apt to note here that electronic forms of transmission is covered by the IT Act, which is a special law. It is settled position in law that a special law shall prevail over the general and prior laws. When the Act in various provisions deals with obscenity in electronic form, it covers the offence under Section 292 IPC.

33. In Jeewan Kumar Raut v. CBI, (2009) 7 SCC 526 in the context of Transplantation of Human Organs Act, 1994 (TOHO) treating it as a special law, the Court held:-

"22. TOHO being a special statute, Section 4 of the Code, which ordinarily would be applicable for investigation into a cognizable offence or the other provisions, may not be applicable. Section 4 provides for investigation, inquiry, trial, etc. according to the provisions of the Code. Sub-section (2) of Section 4, however, specifically provides that offences under any other law shall be investigated, inquired into, tried and otherwise dealt with according to the same provisions, but subject to any enactment for the time being in force regulating the manner or place of investigating, inquiring into, tried or otherwise dealing with such offences.

23. TOHO being a special Act and the matter relating to dealing with offences thereunder having been regulated by reason of the provisions thereof, there cannot be any manner of doubt whatsoever that the same shall prevail over the provisions of the Code." And again:-

"27. The provisions of the Code, thus, for all intent and purport, would apply only to an extent till conflict arises between the provisions of the Code and TOHO and as soon as the area of conflict reaches, TOHO shall prevail over the Code. Ordinarily, thus, although in terms of the Code, the respondent upon completion of investigation and upon obtaining remand of the accused from time to time, was required to file a police report, it was precluded from doing so by reason of the provisions contained in Section 22 of TOHO."

34. In view of the aforesaid analysis and the authorities referred to hereinabove, we are of the considered opinion that the High Court has fallen into error that though charge has not been made out under Section 67 of the IT Act, yet the appellant could be proceeded under Section 292 IPC.

35. Consequently, the appeal is allowed, the orders passed by the High Court and the trial court are set aside and the criminal prosecution lodged against the appellant stands quashed.

Shreya Singhal v Union of India

2015 Indlaw SC 211

Bench: R. F. Nariman, Jasti Chelameswar, Jasti Chelameswar, JJ.

The Judgment was delivered by: R. F. Nariman, J.

1. This batch of writ petitions filed u/art. 32 of the Constitution of India raises very important and far-reaching questions relatable primarily to the fundamental right of free speech and expression guaranteed by Art. 19(1)(a) of the Constitution of India. The immediate cause for concern in these petitions is Section 66A of the Information Technology Act of 2000.

20. With these prefatory remarks, we will now go to the other aspects of the challenge made in these writ petitions and argued before us.

A. Art. 19(1)(a) -

Section 66A has been challenged on the ground that it casts the net very wide - "all information" that is disseminated over the internet is included within its reach.

Two things will be noticed. The first is that the definition is an inclusive one. Second, the definition does not refer to what the content of information can be. In fact, it refers only to the medium through which such information is disseminated. It is clear, therefore, that the petitioners are correct in saying that the public's right to know is directly affected by Section 66A. Information of all kinds is roped in - such information may have scientific, literary or artistic value, it may refer to current events, it may be obscene or seditious. That such information may cause annoyance or inconvenience to some is how the offence is made out. It is clear that the right of the people to know - the market place of ideas - which the internet provides to persons of all kinds is what attracts Section 66A. That the information sent has to be annoying, inconvenient, grossly offensive etc., also shows that no distinction is made between mere discussion or advocacy of a particular point of view which may be annoying or inconvenient or grossly offensive to some and incitement by which such words lead to an imminent causal connection with public disorder, security of State etc. The petitioners are right in saying that Section 66A in creating an offence against persons who use the internet and annoy or cause inconvenience to others very clearly affects the freedom of speech and expression of the citizenry of India at large in that such speech or expression is directly curbed by the creation of the offence contained in Section 66A.

Art. 19(2)

One challenge to Section 66A made by the petitioners' counsel is that the offence created by the said Section has no proximate relation with any of the eight subject matters contained in Art. 19(2). We may incidentally mention that the State has claimed that the said Section can be supported under the heads of public order, defamation, incitement to an offence and decency or morality.

Reasonable Restrictions:

28. As stated, all the above factors may make a distinction between the print and other media as opposed to the internet and the legislature may well, therefore, provide for separate offences so far as free speech over the internet is concerned. There is, therefore, an intelligible differentia having a rational relation to the object sought to be achieved - that there can be creation of offences which are applied to free speech over the internet alone as opposed to other mediums of communication. Thus, an Art. 14 challenge has been repelled by us on this ground later in this judgment. But we do not find anything in the features outlined by the learned Additional Solicitor General to relax the Court's scrutiny of the curbing of the content of free speech over the internet. While it may be possible to narrowly draw a Section creating a new offence, such as Section 69A for instance, relatable only to speech over the internet, yet the validity of such a law will have to be tested on the touchstone of the tests already indicated above.

Public Order

30. In Art. 19(2) (as it originally stood) this sub-head was conspicuously absent. Because of its absence, challenges made to an order made u/s. 7 of the Punjab Maintenance of Public Order Act and to an order made u/s. 9 (1)(a) of the Madras Maintenance of Public Order Act were allowed in two early judgments

by this Court. Thus in Romesh Thappar v. State of Madras, [1950] S.C.R. 594, this Court held that an order made u/s. 9(1)(a) of the Madras Maintenance of Public Order Act (XXIII of 1949) was unconstitutional and void in that it could not be justified as a measure connected with security of the State. While dealing with the expression "public order", this Court held that "public order" is an expression which signifies a state of tranquility which prevails amongst the members of a political society as a result of the internal regulations enforced by the Government which they have established.

35. We have to ask ourselves the question: does a particular act lead to disturbance of the current life of the community or does it merely affect an individual leaving the tranquility of society undisturbed? Going by this test, it is clear that Section 66A is intended to punish any person who uses the internet to disseminate any information that falls within the sub-clauses of Section 66A. It will be immediately noticed that the recipient of the written word that is sent by the person who is accused of the offence is not of any importance so far as this Section is concerned. (Save and except where under sub-cl. (c) the addressee or recipient is deceived or misled about the origin of a particular message.) It is clear, therefore, that the information that is disseminated may be to one individual or several individuals.

The Section makes no distinction between mass dissemination and dissemination to one person. Further, the Section does not require that such message should have a clear tendency to disrupt public order. Such message need not have any potential which could disturb the community at large. The nexus between the message and action that may be taken based on the message is conspicuously absent - there is no ingredient in this offence of inciting anybody to do anything which a reasonable man would then say would have the tendency of being an immediate threat to public safety or tranquility. On all these counts, it is clear that the Section has no proximate relationship to public order whatsoever. The example of a guest at a hotel 'annoying' girls is telling - this Court has held that mere 'annoyance' need not cause disturbance of public order. Under Section 66A, the offence is complete by sending a message for the purpose of causing annoyance, either 'persistently' or otherwise without in any manner impacting public order.

Clear and present danger - tendency to affect.

41. Viewed at either by the standpoint of the clear and present danger test or the tendency to create public disorder, Section 66A would not pass muster as it has no element of any tendency to create public disorder which ought to be an essential ingredient of the offence which it creates.

Defamation

43. It will be noticed that for something to be defamatory, injury to reputation is a basic ingredient. Section 66A does not concern itself with injury to reputation. Something may be grossly offensive and may annoy or be inconvenient to somebody without at all affecting his reputation. It is clear therefore that the Section is not aimed at defamatory statements at all.

Incitement to an offence:

44. Equally, Section 66A has no proximate connection with incitement to commit an offence. Firstly, the information disseminated over the internet need not be information which "incites" anybody at all. Written words may be sent that may be purely in the realm of "discussion" or "advocacy" of a "particular point of view". Further, the mere causing of annoyance, inconvenience, danger etc., or being grossly offensive or having a menacing character are not offences under the Penal Code at all. They may be ingredients of certain offences under the Penal Code but are not offences in themselves. For these reasons, Section 66A has nothing to do with "incitement to an offence". As Section 66A severely curtails information that may be sent on the internet based on whether it is grossly offensive, annoying, inconvenient, etc. and being unrelated to any of the eight subject matters under Art. 19(2) must, therefore, fall foul of Art. 19(1)(a), and not being saved under Art. 19(2), is declared as unconstitutional.

Decency or Morality

47. What has been said with regard to public order and incitement to an offence equally applies here. Section 66A cannot possibly be said to create an offence which falls within the expression 'decency' or 'morality' in that what may be grossly offensive or annoying under the Section need not be obscene at all - in fact the word 'obscene' is conspicuous by its absence in Section 66A.

69. Judged by the standards laid down in the aforesaid judgments, it is quite clear that the expressions used in 66A are completely open-ended and undefined.

70. It will be clear that in all computer related offences that are spoken of by Section 66, mens rea is an ingredient and the expression "dishonestly" and "fraudulently" are defined with some degree of specificity, unlike the expressions used in Section 66A.

71. The provisions contained in Sections 66B up to Section 67B also provide for various punishments for offences that are clearly made out. For example, under Section 66B, whoever dishonestly receives or retains any stolen computer resource or communication device is punished with imprisonment. Under Section 66C, whoever fraudulently or dishonestly makes use of any identification feature of another person is liable to punishment with imprisonment. Under Section 66D, whoever cheats by personating becomes liable to punishment with imprisonment. Section 66F again is a narrowly drawn section which inflicts punishment which may extend to imprisonment for life for persons who threaten the unity, integrity, security or sovereignty of India. Ss. 67 to 67B deal with punishment for offences for publishing or transmitting obscene material including depicting children in sexually explicit acts in electronic form.

Chilling Effect and Overbreadth

83. Information that may be grossly offensive or which causes annoyance or inconvenience are undefined terms which take into the net a very large amount of protected and innocent speech. A person may discuss or even advocate by means of writing disseminated over the internet information that may be a view or point of view pertaining to governmental, literary, scientific or other matters which may be unpalatable to certain sections of society. It is obvious that an expression of a view on any matter may cause annoyance, inconvenience or may be grossly offensive to some. A few examples will suffice. A certain section of a particular community may be grossly offended or annoyed by communications over the internet by "liberal views" - such as the emancipation of women or the abolition of the caste system or whether certain members of a non proselytizing religion should be allowed to bring persons within their fold who are otherwise outside the fold. Each one of these things may be grossly offensive, annoying, inconvenient, insulting or injurious to large sections of particular communities and would fall within the net cast by Section 66A. In point of fact, Section 66A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of the Section and if it is to withstand the test of Constitutionality, the chilling effect on free speech would be total.

86. That the content of the right under Art. 19(1)(a) remains the same whatever the means of communication including internet communication is clearly established by Reno's case (supra) and by The Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal & Anr., (1995) SCC 2 161 1995 Indlaw SC 2353 already referred to. **It is thus clear that not only are the expressions used in Section 66A expressions of inexactitude but they are also over broad and would fall foul of the repeated injunctions of this Court that restrictions on the freedom of speech must be couched in the narrowest possible terms.**

Possibility of an act being abused is not a ground to test its validity:

92. If Section 66A is otherwise invalid, it cannot be saved by an assurance from the learned Additional Solicitor General that it will be administered in a reasonable manner. Governments may come and Governments may go but Section 66A goes on forever. An assurance from the present Government even if carried out faithfully would not bind any successor Government. It must, therefore, be held that Section 66A must be judged on its own merits without any reference to how well it may be administered.

Severability:

95. It has been held by us that Section 66A purports to authorize the imposition of restrictions on the fundamental right contained in Art. 19(1) (a) in language wide enough to cover restrictions both within and without the limits of Constitutionally permissible legislative action. We have held following K.A. Abbas' case that the possibility of Section 66A being applied for purposes not sanctioned by the Constitution cannot be ruled out. It must, therefore, be held to be wholly unconstitutional and void.

96. The present being a case of an Art. 19(1)(a) violation, Romesh Thappar's judgment would apply on all fours. In an Art. 19(1)(g) challenge, there is no question of a law being applied for purposes not

sanctioned by the Constitution for the simple reason that the eight subject matters of Art. 19(2) are conspicuous by their absence in Art. 19(6) which only speaks of reasonable restrictions in the interests of the general public. The present is a case where, as has been held above, Section 66A does not fall within any of the subject matters contained in Art. 19(2) and the possibility of its being applied for purposes outside those subject matters is clear. We therefore hold that no part of Section 66A is severable and the provision as a whole must be declared unconstitutional.

Article 14

98. We have already held that Section 66A creates an offence which is vague and overbroad, and, therefore, unconstitutional under Art. 19(1)(a) and not saved by Art. 19(2). We have also held that the wider range of circulation over the internet cannot restrict the content of the right under Art. 19(1)(a) nor can it justify its denial. However, when we come to discrimination under Article 14, we are unable to agree with counsel for the petitioners that there is no intelligible differentia between the medium of print, broadcast and real live speech as opposed to speech on the internet. The intelligible differentia is clear - the internet gives any individual a platform which requires very little or no payment through which to air his views. The learned Additional Solicitor General has correctly said that something posted on a site or website travels like lightning and can reach millions of persons all over the world. If the petitioners were right, this Art. 14 argument would apply equally to all other offences created by the Information Technology Act which are not the subject matter of challenge in these petitions. We make it clear that there is an intelligible differentia between speech on the internet and other mediums of communication for which separate offences can certainly be created by legislation. We find, therefore, that the challenge on the ground of Art. 14 must fail.

Procedural Unreasonableness

99. One other argument must now be considered. According to the petitioners, Section 66A also suffers from the vice of procedural unreasonableness. In that, if, for example, criminal defamation is alleged, the safeguards available u/s. 199 Cr.P.C. would not be available for a like offence committed under Section 66A. Such safeguards are that no court shall take cognizance of such an offence except upon a complaint made by some person aggrieved by the offence and that such complaint will have to be made within six months from the date on which the offence is alleged to have been committed. Further, safeguards that are to be found in Ss. 95 and 96 of the Cr.P.C. are also absent when it comes to Section 66A. For example, where any newspaper book or document wherever printed appears to contain matter which is obscene, hurts the religious feelings of some community, is seditious in nature, causes enmity or hatred to a certain section of the public, or is against national integration, such book, newspaper or document may be seized but u/s. 96 any person having any interest in such newspaper, book or document may within two months from the date of a publication seizing such documents, books or newspapers apply to the High court to set aside such declaration. Such matter is to be heard by a Bench consisting of at least three Judges or in High Courts which consist of less than three Judges, such special Bench as may be composed of all the Judges of that High Court.

100. It is clear that Ss. 95 and 96 of the Criminal Procedure Code reveal a certain degree of sensitivity to the fundamental right to free speech and expression. If matter is to be seized on specific grounds which are relatable to the subject matters contained in Art. 19(2), it would be open for persons affected by such seizure to get a declaration from a High Court consisting of at least three Judges that in fact publication of the so-called offensive matter does not in fact relate to any of the specified subjects contained in Art. 19(2).

101. Again, for offences in the nature of promoting enmity between different groups on grounds of religion etc. or offences relatable to deliberate and malicious acts intending to outrage religious feelings or statements that create or promote enmity, hatred or ill-will between classes can only be taken cognizance of by courts with the previous sanction of the Central Government or the State Government. This procedural safeguard does not apply even when a similar offence may be committed over the internet where a person is booked under Section 66A instead of the aforesaid Sections.

Having struck down Section 66A on substantive grounds, we need not decide the procedural unreasonableness aspect of the Section.

S. 118 of the Kerala Police Act.

102. Learned counsel for the Petitioner in Writ Petition No. 196 of 2014 assailed sub-section (d) of S. 118.

The Kerala Police Act as a whole would necessarily fall under Entry 2 of List II. In addition, S. 118 would also fall within Entry 1 of List II in that as its marginal note tells us it deals with penalties for causing grave violation of public order or danger.

104. It is well settled that a statute cannot be dissected and then examined as to under what field of legislation each part would separately fall.

105. It is, therefore, clear that the Kerala Police Act as a whole and S. 118 as part thereof falls in pith and substance within Entry 2 List II, notwithstanding any incidental encroachment that it may have made on any other Entry in List I. Even otherwise, the penalty created for causing annoyance in an indecent manner in pith and substance would fall within Entry 1 List III which speaks of criminal law and would thus be within the competence of the State Legislature in any case.

106. However, what has been said about Section 66A would apply directly to S. 118(d) of the Kerala Police Act, as causing annoyance in an indecent manner suffers from the same type of vagueness and over breadth, that led to the invalidity of Section 66A, and for the reasons given for striking down Section 66A, S. 118(d) also violates Art. 19(1)(a) and not being a reasonable restriction on the said right and not being saved under any of the subject matters contained in Art. 19(2) is hereby declared to be unconstitutional.

Section 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

107. Section 69A of the Information Technology Act has already been set out in paragraph 2 of the judgment. Under sub-s. (2) thereof, the 2009 Rules have been framed. Under Rule 3, the Central Government shall designate by notification in the official gazette an officer of the Central Government not below the rank of a Joint Secretary as the Designated Officer for the purpose of issuing direction for blocking for access by the public any information referable to Section 69A of the Act. Under Rule 4, every organization as defined under Rule 2(g), (which refers to the Government of India, State Governments, Union Territories and agencies of the Central Government as may be notified in the Official Gazette by the Central Government)- is to designate one of its officers as the "Nodal Officer". Under Rule 6, any person may send their complaint to the "Nodal Officer" of the concerned Organization for blocking, which complaint will then have to be examined by the concerned Organization regard being had to the parameters laid down in Section 69A(1) and after being so satisfied, shall transmit such complaint through its Nodal Officer to the Designated Officer in a format specified by the Rules. The Designated Officer is not to entertain any complaint or request for blocking directly from any person. Under Rule 5, the Designated Officer may on receiving any such request or complaint from the Nodal Officer of an Organization or from a competent court, by order direct any intermediary or agency of the Government to block any information or part thereof for the reasons specified in 69A(1). Under Rule 7 thereof, the request/complaint shall then be examined by a Committee of Government Personnel who under Rule 8 are first to make all reasonable efforts to identify the originator or intermediary who has hosted the information.

If so identified, a notice shall issue to appear and submit their reply at a specified date and time which shall not be less than 48 hours from the date and time of receipt of notice by such person or intermediary. The Committee then examines the request and is to consider whether the request is covered by 69A(1) and is then to give a specific recommendation in writing to the Nodal Officer of the concerned Organization. It is only thereafter that the Designated Officer is to submit the Committee's recommendation to the Secretary, Department of Information Technology who is to approve such requests or complaints. Upon such approval, the Designated Officer shall then direct any agency of Government or intermediary to block the offending information. Rule 9 provides for blocking of information in cases of emergency where delay caused would be fatal in which case the blocking may take place without any opportunity of hearing. The Designated Officer shall then, not later than 48 hours of the issue of the interim direction, bring the request before the Committee referred to earlier, and only on the recommendation of the Committee, is the Secretary Department of Information Technology to pass the final order. Under Rule 10, in the case of an order of a competent court in India, the Designated Officer shall, on receipt of a certified copy of a court order, submit it to the Secretary, Department of

Information Technology and then initiate action as directed by the Court. In addition to the above safeguards, under Rule 14 a Review Committee shall meet at least once in two months and record its findings as to whether directions issued are in accordance with Section 69A(1) and if it is of the contrary opinion, the Review Committee may set aside such directions and issue orders to unblock the said information. Under Rule 16, strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof.

109. It will be noticed that Section 69A unlike Section 66A is a narrowly drawn provision with several safeguards. First and foremost, blocking can only be resorted to where the Central Government is satisfied that it is necessary so to do. Secondly, such necessity is relatable only to some of the subjects set out in Art. 19(2). Thirdly, reasons have to be recorded in writing in such blocking order so that they may be assailed in a writ petition u/art. 226 of the Constitution.

110. The Rules further provide for a hearing before the Committee set up - which Committee then looks into whether or not it is necessary to block such information. It is only when the Committee finds that there is such a necessity that a blocking order is made. It is also clear from an examination of Rule 8 that it is not merely the intermediary who may be heard. If the "person" i.e. the originator is identified he is also to be heard before a blocking order is passed. Above all, it is only after these procedural safeguards are met that blocking orders are made and in case there is a certified copy of a court order, only then can such blocking order also be made. It is only an intermediary who finally fails to comply with the directions issued who is punishable under sub-s. (3) of Section 69A.

111. Merely because certain additional safeguards such as those found in S. 95 and 96 CrPC are not available does not make the Rules Constitutionally infirm. We are of the view that the Rules are not Constitutionally infirm in any manner.

S. 79 and the Information Technology (Intermediary Guidelines) Rules, 2011.

112. S. 79 belongs to Chapter XII of the Act in which intermediaries are exempt from liability if they fulfill the conditions of the Section.

113. Under the 2011 Rules, by Rule 3 an intermediary has not only to publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource but he has also to inform all users of the various matters set out in Rule 3(2).

116. It must first be appreciated that S. 79 is an exemption provision. Being an exemption provision, it is closely related to provisions which provide for offences including Section 69A. We have seen how under Section 69A blocking can take place only by a reasoned order after complying with several procedural safeguards including a hearing to the originator and intermediary. We have also seen how there are only two ways in which a blocking order can be passed - one by the Designated Officer after complying with the 2009 Rules and the other by the Designated Officer when he has to follow an order passed by a competent court. The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69A read with 2009 Rules.

117. S. 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject matters laid down in Art. 19(2). Unlawful acts beyond what is laid down in Art. 19(2) obviously cannot form any part of S. 79. With these two caveats, we refrain from striking down S. 79(3)(b).

119. In conclusion, we may summarise what has been held by us above:

Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Art. 19(1)(a) and not saved under Art. 19(2).

Section 69A and the Information Technology (Procedure & Safeguards for Blocking for Access of

Information by Public) Rules 2009 are Constitutionally valid.

S. 79 is valid subject to S. 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Art. 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Similarly, the Information Technology "Intermediary Guidelines" Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment.

S. 118(d) of the Kerala Police Act is struck down being violative of Art. 19(1)(a) and not saved by Art. 19(2).

Sanjay Kumar Kedia v Narcotics Control Bureau

2007(13) SCALE 631

Bench: H.S. Bedi, S.B. Sinha, JJ.

The Judgment was delivered by: Harjit Singh Bedi, J.

2. The appellant Sanjay Kumar Kedia, a highly qualified individual, set up two companies M/s. Xponse Technologies Limited (XTL) and M/s. Xponse IT Services Pvt. Ltd. (XIT) on 22.4.2002 and 8.9.2004 respectively which were duly incorporated under the Indian Companies Act, 1956. On 1.2.2007 officers of the Narcotics Control Bureau (NCB) conducted a search at the residence and office premises of the appellant but found nothing incriminating. He was also called upon to appear before the NCB on a number of occasions pursuant to a notice issued to him u/s. 67 of the Narcotic Drugs and Psychotropic Substances Act, 1985 ("the Act") and was ultimately arrested and the bank accounts and premises of the two companies were also seized or sealed. On 13.3.2007 the appellant filed an application for bail in the High Court which was dismissed on the ground that a prima facie case u/ss. 24 and 29 of the Act had been made out and that the investigation was yet not complete.

The appellant thereafter moved a second bail application before the High Court on 16.4.2007 which too was dismissed with the observations that the enquiry was at a critical stage and that the department should be afforded sufficient time to conduct its enquiry and to bring it to its logical conclusion as the alleged offences had widespread ramifications for society. It appears that a bail application was thereafter filed by the appellant before the Special Judge which too was rejected on 28.5.2007 with the observations that the investigation was still in progress. Aggrieved thereby, the appellant preferred yet another application for bail before the High Court on 4.6.2007 which too was dismissed on 7.6.2007. The present appeal has been filed against this order.

3. Notice was issued on the Special Leave Petition on 30.7.2007 by a Division Bench noticing a contention raised by Mr. Tulsi that service providers such as the two companies which were intermediaries were protected from prosecution by S. 79 of the Information Technology Act, 2000. An affidavit in reply has also been filed on behalf of the respondent NCB and a rejoinder affidavit in reply thereto by the appellant.

5. Mr. Tulsi has first and foremost argued that the allegations against the appellant were that he had used the network facilities provided by his companies for arranging the supply of banned psychotropic substances on line but there was no evidence to suggest that the appellant had been involved in dealing with psychotropic substances or engaged in or controlled any trade whereby such a substance obtained outside India had been supplied to persons outside India and as such no case u/s. 24 of the Act had been made out against the appellant. Elaborating this argument, he has submitted that the two drugs which the appellant had allegedly arranged for supply were phentermine and butalbital and as these drugs were not included in Schedule-I of the Narcotic Drugs or Psychotropic Substances Rules 1987 in terms of the notification dated 21.2.2003 and were also recognized by the Control Substances Act, a law applicable in the United States, as having low potential for misuse and it was possible to obtain these drugs either on written or oral prescription of a doctor, the supply of these drugs did not fall within the mischief of S. 24. He has further argued that in the circumstance, the companies were mere network service providers they were protected under S. 79 of the Technology Act from any prosecution.

6. Mr. Vikas Singh, the learned Additional Solicitor General for the respondents has however pointed out that the aforesaid drugs figured in the Schedule appended to the Act pertaining to the list of psychotropic substances (at Srl. Nos. 70 and 93) and as such it was clear that the two drugs were psychotropic substances and therefore subject to the Act. It has also been pointed out that the appellant had been charged for offences u/ss. 24 and 29 of the Act which visualized that a person could be guilty without personally handling a psychotropic substance and the evidence so far collected showed that the appellant was in fact a facilitator between buyers and certain pharmacies either owned or controlled by him or associated with the two companies and that S. 79 of the Technology Act could not by any stretch of imagination guarantee immunity from prosecution under the provisions of the Act.

7. It is clear from the Schedule to the Act that the two drugs phentermine and butalbital are psychotropic substances and therefore fall within the prohibition contained in S. 8 thereof. The appellant has been charged for offences punishable u/ss. 24 and 29 of the Act.

A perusal of S. 24 would show that it deals with the engagement or control of a trade in Narcotic Drugs and Psychotropic Substances controlled and supplied outside India and S. 29 provides for the penalty arising out of an abetment or criminal conspiracy to commit an offence under Chapter IV which includes S. 24. We have accordingly examined the facts of the case in the light of the argument of Mr. Tulsi that the companies only provided third party data and information without any knowledge as to the commission of an offence under the Act. We have gone through the affidavit of Shri A.P. Siddiqui Deputy Director, NCB and reproduce the conclusions drawn on the investigation, in his words.

"(i) The accused and its associates are not intermediary as defined u/s. 79 of the said Act as their acts and deeds was not simply restricted to provision of third party data or information without having knowledge as to commission of offence under the NDPS Act. *The company (Xponse Technologies Ltd. And Xpose IT Services Pvt. Ltd. Headed by Sanjay Kedia) has designed, developed, hosted the pharmaceutical websites and was using these websites, huge quantity of psychotropic substances (Phentermine and Butalbital) have been distributed in USA with the help of his associates. Following are the online pharmacy websites which are owned by Xponse or Sanjay Kedia.*

(1) Brother Pharmacy.com and LessRx.com: Brothers pharmacy.com, online pharmacy was identified as a marketing website (front end) for pharmaceutical drugs. LessRx.com has been identified as a "back end" site which was being utilized to process orders for pharmaceutical drugs through Brotherspharmacy.com. LessRx.com's registrant and administrative contact was listed True Value Pharmacy located at 29B, Rabindra Sarani, Kolkata, India-700073. Telephone No.033-2335-7621 which is the address of Sanjay Kedia. LessRx.com's IP address is 203.86.100.95. The following websites were also utilizing this IP address:

ALADIESPHARMACY.com, EXPRESSPHENTERMINE.com, FAMILYYONLINEPHARMACY.com ONLINEEXPRESSPHARMACY.com, SHIPPEDLIPITOR.com Domain name Servers for LessRx.com (IP address: 203.86.100.95) were NS.PALCOMONLINE.com and NS2PALCOMLINE.com.

The LessRx.com's website hosting company was identified as Pacom Web Pvt Ltd, C-56/14,1st Floor, Institutional Area, Sector 62, Noida-201301. Sanjay Kedia entrusted the hosting work to Palcom at VSNL, Delhi. These servers have been seized. Voluntary statement of Shri Ashish Chaudhary, Prop. Of Palcom Web Pvt Ltd.indicates that He maintained the websites on behal of Xponse.

According to the bank records, funds have been wired from Brothers pharmacy, Inc's Washington Mutual Bank Account #0971709674 to Xponse IT services Pvt Ltd, ABN AMRO bank account No.1029985, Kolkata.

(2) Deliveredmedicine.com : A review of the Xponse's website-XPONSEIT.com was conducted and observed and advertisement for XPONSERX. That XPONSERX was described as a software platform developed for the purpose of powering online pharmacies. Xponserx was designed to process internet pharmacy orders by allowing customers to order drugs. Drug Enforcement Administration (DEA), USA conducted a "whois" reverse lookup on domain name XPONSERX.COM was at domaintools.Com and it revealed that XPONSERX.COM was registered to Xponse IT Services Pvt Ltd, Sanjay kedia, 29B,Rabindra Sarani, 12E,3rd floor, Kolkata, WB 70073. Telephone no.+91- 9830252828 was also provided for Xponse. Two websites were featured on the XPONSEIT.COM websites as featured clients. And these were DELIVEREDMEDICINE.COM AND TRUEVALUEPRESCRIPTIONS.COM. Review indicated that these two websites were internet pharmacies.

Consequently a "whois" reverse look-up on domain name DELIVEREDMEDICINE.COM at domainstools.com conducted by DEA revealed that it was registered to Xponse Inc.,2760 Park Ave.,Santa Clara, CA, USA which is the address of Sanjay Kedia.

(3) Truevalueprescriptions.com: Review of this website indicated that this website was a internet pharmacy. In addition TRUEVALUEPRESCRIPTIONS listed Phentermine as a drug available for sale. It appeared that orders for drugs could be made without a prescription from the TRUEVALUE website, it was noted that orders for drugs could be placed without seeing a doctor. According to the website, a customer can complete an online questionnaire when placing the order for a drug in lieu of a physical exam in a physician's office. Toll free telephone number 800-590-5942 was provided on the TRUEVALUE website for customer Service.

DEA, conducted a "whois" reverse look-up on domain name TRUEVALUEPRESCRIPTIONS.COM at

domaintools.com and revealed that IP address was 203.86.100.76 and the server that hosts the website was located at Palcom, Delhi which also belongs to Xponse.

From the above facts it is clear that the Xponse Technologies Ltd and Xponse IT Services Pvt Ltd were not acting merely as a network service provider but were actually running internet pharmacy and dealing with prescription drugs like Phentermine and Butalbital."

8. We thus find that the appellant and his associates were not innocent intermediaries or network service providers as defined u/s. 79 of the Technology Act but the said business was only a facade and camouflage for more sinister activity. In this situation, S. 79 will not grant immunity to an accused who has violated the provisions of the Act as this provision gives immunity from prosecution for an offence only under Technology Act itself.

9. We are therefore of the opinion that in the face of overwhelming inculpatory evidence it is not possible to give the finding envisaged u/s. 37 of the Act for the grant of bail that there were reasonable grounds for believing that the appellant was not guilty of the offence alleged, or that he would not resume his activities should bail be granted.

10. For the reasons recorded above, we find no merit in this appeal, which is accordingly dismissed. We however qualify that the observations made above are in the context of the arguments raised by the learned counsel on the bail matter which obligated us to deal with them, and will not influence the proceedings or decision in the trial in any manner. Appeal dismissed.

……

Dr. Rini Johar v State of Madhya Pradesh

AIR 2016 SC 2679

Bench: Dipak Misra, Shiva Kirti Singh, JJ.

The Judgment was delivered by: Dipak Misra, J.

1. The petitioner no.1 is a doctor and she is presently pursuing higher studies in United States of America (USA). Petitioner no.2, a septuagenarian lady, is a practicing Advocate in the District Court at Pune for last 36 years. Petitioner no.1 is associated with M/s. Progen, a US company.

2. As the facts would unveil, the informant, respondent no.8 herein, had sent an email to the company for purchase of machine Aura Cam, 6000, which is an Aura Imaging Equipment, in India and the concerned company sent an email to the respondent making a reference to the petitioner no.1. Thereafter, the said respondent sent an email asking her to send the address where he could meet her and have details for making payment. He also expressed his interest to become a distributor.

3. The informant visited the petitioner no.1 at Pune and received a demo of Aura Cam 6000 and being satisfied decided to purchase a lesser price machine i.e. "Twinaura Pro" for a total sum of Rs.2,54,800/-. He paid a sum of Rs.2,50,000/- for which a hand written receipt was given as the proof of payment. During the course of the said meeting, the 8th respondent expressed his desire to purchase a laptop of M/s. Progen of which the petitioner no. 1 was the representative. In pursuance of the discussion, the laptop was given to him who acknowledged it by stating that he owed a sum of Rs.4,800/- as balance consideration towards the Aura Cam and an amount of USD 350 towards the laptop. An assurance was given for remitting the money within a short time. As averred, the respondent no.8 had never raised any grievance relating either to the machine or the laptop. Certain transactions between the informant and the US company have been mentioned and the allegations have been made against the 8th respondent that he represented himself as the sole distributor in India which was brought to the notice of the concerned police in the State of M.P. by the competent authority of the company. The said facts really do not have much relevance to the lis which we are going to adjudicate in the present writ petition.

4. When the matter stood thus, the respondent no.8 filed a complaint before the Inspector General of Police, Cyber Cell, Bhopal alleging that the petitioner no.1 and Mr. Guy Coggin had committed fraud of US 10,500. On the basis of the complaint made, FIR no. 24/2012 under Section 420 and 34 of the Indian Penal Code (IPC) and Section 66-D of the Information Technology Act, 2000 (for brevity, 'the Act') was registered against the petitioners by Cyber Police Headquarters, Bhopal, M.P. The respondent no.2, I.G. Cyber Cell, issued an order on 20.11.2012 which is to the following effect:-

"Cyber state police having registered FIR 24/2012 under S 420, 34 of Indian Penal Code *and 66 D of* IT Act *search and information the undersigned persons are asked to go to Pune.*

1. R.R. Devendra Sisodia
2. R.R. (Lady) Ishrat Praveen Khan
3. RR (Lady) Valari Upadhyay"

5. On 21.11.2012, Dy. S.P. State Cyber Police, Bhopal proceeded to pass the following order:-

"Cyber state police having registered FIR 24/2012 under S 420, 34 Indian Penal Code *and S 66 D of* IT Act *accused Rini Johar and Gulshan Johar should be arrested and for that lady constable Ishrat Khan has been deputed with case diary with address from where they are to be found and arrested and it is ordered that they be brought to Bhopal. In reference to which you have been given possession of the said case diary."*

7. As the narration would unfurl, on 27.11.2012, the petitioners were arrested from their residence at Pune. Various assertions have been made as regards the legality of the arrest which cover the spectrum of non-presence of the witnesses at the time of arrest of the petitioners, non-mentioning of date, and arrest by unauthorized officers, etc. It is also asserted after they were arrested, they were taken from Pune to Bhopal in an unreserved railway compartment marked - 'viklang' (handicapped). Despite request, the petitioner no.2, an old lady, was not taken to a doctor, and was compelled to lie on the cold floor of the train compartment without any food and water. Indignified treatment and the humiliation faced by the petitioners have been mentioned in great detail. On 28.11.2012, they were produced before the learned Magistrate at Bhopal and the petitioner no. 2 was enlarged on bail after being in custody for about 17 days

and the petitioner no.1 was released after more than three weeks. There is allegation that they were forced to pay Rs.5 lakhs to respondent no.3, Deepak Thakur, Dy. S.P. Cyber Cell, Bhopal. On 18.12.2012, chargesheet was filed and thereafter a petition under Section 482 CrPC has been filed before the High Court for quashment of the FIR.

8. At this stage, it is pertinent to state that on 19.2.2015 the petitioners filed an application for discharge and the learned Magistrate passed an order discharging the petitioners in respect of the offence punishable under Section 66-D of the Act. However, learned Magistrate has opined that there is prima facie case for the offence punishable under Section 66-A(b) of the Act read with Section 420 and 34 of the IPC.

10. In this writ petition, first we shall address to the challenge relating to the validity and legality of arrest, advert to the aspect whether the petitioners would be entitled to any compensation on the bedrock of public law remedy and thereafter finally to the justifiability of the continuance of the criminal proceedings. Be it stated here that this Court on 7.12.2015, taking note of the submissions of the petitioners that they are not interested to prosecute their petition under Section 482 CrPC directed that the said petition is deemed to have been disposed of. It is also requisite to note here that despite efforts being made by the petitioners as well as the State of M.P, respondent no.8, who belongs to Jabalpur, M.P. could not be served. This Court is inclined to infer that the said respondent is really not interested to appear and contest.

12. We consider it imperative to refer to the enquiry made by the State and the findings arrived at by the enquiry officer. It is asserted in the counter affidavit that the petitioners had made a complaint to the Lokayukta Police (M.P. Special Police Establishment) alleging that Deepak Thakur, respondent no.3 herein, demanded a bribe of Rs.10 lakhs for letting them go and pursuant to the said demand, initially a sum of Rs.2,50,000/- was paid and subsequently a sum of Rs.2,50,000/- was also given. The Lokayukta Police had already registered a preliminary enquiry no. 33/2015 and after enquiry submitted an enquiry report dated 18.6.2015 stating that prima facie case had been made out against Deepak Thakur, Dy. S.P., Cyber Cell, Bhopal, Ishrat Khan, Head Constable, Cyber Cell, Bhopal, Inderpal, Writer, Cyber Cell Bhopal and Saurabh Bhat, Clerk, Cyber Cell, Bhopal under Section 13(1)(d) and Section 13(2) of the Prevention of Corruption Act, 1988 and Section 120B IPC. Based on the said preliminary enquiry report, FIR No. 273/2015 dated 27.3.2015 has been registered against the accused persons in respect of the said offences and further steps under the CrPC are being taken. Be it clarified, we are not at all concerned with the launching of said prosecution and accordingly we shall not advert to the same.

13. It is perceivable that the State in its initial affidavit had stated that the Director General of Police by its order dated 8.7.2015 had appointed Inspector General of Police, CID to enquire into the allegations as regards the violation of the provisions enshrined under Section 41-A to 41-C of CrPC. It needs to be stated here that in pursuance of the order passed by the Director General, an enquiry has been conducted by Inspector General of Police Administration, CID, Bhopal. It has been styled as "preliminary enquiry". The said report dated 19.08.2015 has been brought on record. The Inquiring Authority has recorded the statement of Ms. Ishrat Praveen Khan. The part of her statement reads as follows:-

"... When I received the order, I requested DSP Shri Deepak Thakur that I was not in the District Police Force. I do not have any knowledge about IPC/Cr.P.C./Police Regulation/Police Act *and* Evidence Act, IT Act *as I have not obtained any training in Police Training School, nor do I have any knowledge in this regard, nor do I have any knowledge to fill up the seizure memo and arrest memo. Even after the request, DSP Shri Deepak Thakur asked in strict word that I must follow the order. The duty certificate was granted to me on 26.11.2012, on which Report No.567 time 16.30 was registered, in which there are clear directions. In compliance with this order, we reached Kondwa Police Station in Pune Maharashtra on 27.11.2012 with my team and 2 constables and 1 woman constable were sent to assist us from there. The persons of the police station Kondwa came to know reaching Lulla Nagar that the said area does not fall under their police station area so the police of Kondwa phoning Banwari Police Station got to bring the force for help Banwari Police Station. I had given the written application in PS Banwari. The entire team reached the house of Rini Johar and 01 laptop of Dell Company and 1 data card of Reliance Company were seized. Rini Johar called her mother Gulshan Johar from the Court furnishing information to her about her custody. Thereafter, Shri Rini Johar had called up the Inspector General of Police, State Cyber Police Shri Anil Kumar Gupta. I and my team had taken Miss Rini Johar and Smt. Gulshan in our custody. I and Constable Miss Hemlata Jharbare conduced robe search of Miss Rini*

Johar and Smt. Gulshan Johar. Nothing was found on their body."

14. He has also recorded the statement of Devender Sisodia, Ms. Vallari Upadhyay, Ms. Hemlata Jharbare and thereafter recorded his findings. The findings arrived at in the preliminary enquiry read thus:-

"24. Finding of the preliminary inquiry:- It was found during the preliminary enquiry that Crime No.24/12 had been registered after the inquiry of one written complaint of the applicant Shri Vikram Rajput, but this complaint inquiry report during the investigation of the offence has been kept as the relevant evidence. The crime was registered on 27.11.2012 under Section 420, 34 IPC *read with Section 66D* IT Act, 2000 *against the named accused persons. The offence was to the effect that though the alleged accused persons obtained Rs.5.00 lakh, they did not supply the camera etc and they supplied the defective articles. This sale - purchase was conducted through the online correspondence, due to which the section of* IT Act *was imposed. It was found on the preliminary inquiry that Shri Vikram Rajput gave the payment of Rs.2.50 lakh by the bank draft and the remaining payment by cash. The facts of the payment and supply are now disputed and the trial of Crime No.24/12 is pending in the competent Court. Therefore, to give any inquiry finding on it would not be proper. It is clear from the documents attached to the case diary and the statement of Shri Deepak Thakur that Shri Deepak Thakur sent 2 notices respectively by the post and through the Deputy Commissioner, Economic Crime and Cyber Pune respectively to Miss Rini Johar on 01.06.2012 and 02.07.2012 in the investigation of the offence, but they did not appear before the Investigator. It has not been written above both the notices if the notice has been issued under Section 41A of* Cr.P.C. *It is also not clear whether or not these both notices were severed to Miss Rini Johar.*

25. This case is related to the alleged cheating between two persons in respect of sale and purchase of goods. The maximum sentence in Section 420 is the period upto 7 years and similarly when the reasons mentioned in Section 41 (1)(B) are not found, the suspects of the crime should be made to appear for the interrogation in the investigation issuing notice to them. Justice Late Krishna Ayyer has held in Jolly George Varghese v. Bank of Cochin AIR 1980 SC 470 that "No one shall be imprisoned merely on the ground of inability to fulfill a contractual obligation". Section 41(2) of Cr.P.C. *grants power to the Investigator that if the suspect does not appear for the investigation despite the notice, he can be arrested, though this reason having been mentioned in the case diary should have been produced before the Magistrate, but no reason for the arrest has been mentioned in the case diary. No notice has been sent to the old woman Smt. Gulshan Johar (aged about 70 years), nor has she played any role in committing any offence. Only the draft of Rs.2.50 lakh had been deposited in her account. No binding ground has been mentioned in respect of her arrest in the case diary."*

And again:-

"28. It has not been mentioned anywhere in the arrest memo and case diary that the information of the arrest of both women was furnished to any of their relatives and friends. It has become clear from the statements that when both the women were arrested physically they were brought to PS Banwari Pune, where the arrest memo was prepared. There is the signature of Shri Amol Shetty as the witness of the seizure memo. Shri Deepak Thakur has stated in his statement that the handwriting of the seizure memo is of the constable Shri Indrapal. Shri Indrapal did not go as a member of the arresting persons to Pune. The seizure memo does not have the signature of Amol Shetty as well, which proves prima facie that the seizure memo was not prepared on 27.11.2012 in Pune. The report no.29/12 dated 27.11.2012 of seeking police help in PS Banwari is recorded, but no information is recorded at the police station that MP Police are taking by arresting these citizens with them. As a result, the information of the arrested persons was neither furnished in the District Police Control Room Pune, nor was it published there. It has also been clarified in the preliminary inquiry that the accused persons after they were arrested were not produced before the Local Judge and they were brought to Bhopal by rail. Miss Ishrat Khan stated that she did not obtain the rail warrant of neither the policepersons nor the accused during return due to paucity of time."

And finally:-

"As such, the facts of arresting both the suspected women and making seizure memo searching their houses not fully following the procedure of arrest by the Investigator and police team have come to the fore in the preliminary enquiry prima facie."

15. Keeping the aforesaid facts in view, we may refer to the decisions in the field and the submissions canvassed by Mr. Fernandes, learned Amicus Curiae.

18. In D.K. Basu v. State of W.B. (1997) 1 SCC 416 1996 Indlaw SC 1546, after referring to the authorities in Joginder Kumar 1994 Indlaw SC 1505 (supra), Nilabati Behera v. State of Orissa (1993) 2 SCC 746 1993 Indlaw SC 999 and State of M.P. v. Shyamsunder Trivedi (1995) 4 SCC 262 1995 Indlaw SC 1216 the Court laid down certain guidelines to be followed in cases of arrest and detention till legal provisions are made in that behalf as preventive measures.

19. Mr. Fernandes, learned Amicus Curiae, in a tabular chart has pointed that none of the requirements had been complied with. Various reasons have been ascribed for the same. On a scrutiny of enquiry report and the factual assertions made, it is limpid that some of the guidelines have been violated. It is strenuously urged by Mr. Fernandes that Section 66-A(b) of the Information Technology Act, 2000 provides maximum sentence of three years and Section 420 CrPC stipulates sentence of seven years and, therefore, it was absolutely imperative on the part of the arresting authority to comply with the procedure postulated in Section 41-A of the Code of Criminal Procedure.

22. We have referred to the enquiry report and the legal position prevalent in the field. On a studied scrutiny of the report, it is quite vivid that the arrest of the petitioners was not made by following the procedure of arrest. Section 41-A CrPC as has been interpreted by this Court has not been followed. The report clearly shows there have been number of violations in the arrest, and seizure. Circumstances in no case justify the manner in which the petitioners were treated.

23. In such a situation, we are inclined to think that the dignity of the petitioners, a doctor and a practicing Advocate has been seriously jeopardized. Dignity, as has been held in Charu Khurana v. Union of India (2015) 1 SCC 192, is the quintessential quality of a personality, for it is a highly cherished value. It is also clear that liberty of the petitioner was curtailed in violation of law. The freedom of an individual has its sanctity. When the individual liberty is curtailed in an unlawful manner, the victim is likely to feel more anguished, agonized, shaken, perturbed, disillusioned and emotionally torn. It is an assault on his/her identity. The said identity is sacrosanct under the Constitution. Therefore, for curtailment of liberty, requisite norms are to be followed. Fidelity to statutory safeguards instil faith of the collective in the system. It does not require wisdom of a seer to visualize that for some invisible reason, an attempt has been made to corrode the procedural safeguards which are meant to sustain the sanguinity of liberty. The investigating agency, as it seems, has put its sense of accountability to law on the ventilator. The two ladies have been arrested without following the procedure and put in the compartment of a train without being produced before the local Magistrate from Pune to Bhopal. One need not be Argus - eyed to perceive the same. Its visibility is as clear as the cloudless noon day.

25. Having held thus, we shall proceed to the facet of grant of compensation. The officers of the State had played with the liberty of the petitioners and, in a way, experimented with it. Law does not countenance such kind of experiments as that causes trauma and pain.

27. In the case at hand, there has been violation of Article 21 and the petitioners were compelled to face humiliation. They have been treated with an attitude of insensibility. Not only there are violation of guidelines issued in the case of D.K. Basu 1996 Indlaw SC 1546 (supra), there are also flagrant violation of mandate of law enshrined under Section 41 and Section 41-A of CrPC. The investigating officers in no circumstances can flout the law with brazen proclivity. In such a situation, the public law remedy which has been postulated in Nilawati Behra 1993 Indlaw SC 999 (supra), Sube Singh v. State of Haryana (2006) 3 SCC 178, Hardeep Singh v. State of M.P. (2012) 1 SCC 748, comes into play. The constitutional courts taking note of suffering and humiliation are entitled to grant compensation. That has been regarded as a redeeming feature. In the case at hand, taking into consideration the totality of facts and circumstances, we think it appropriate to grant a sum of Rs.5,00,000/- (rupees five lakhs only) towards compensation to each of the petitioners to be paid by the State of M.P. within three months hence. It will be open to the State to proceed against the erring officials, if so advised.

28. The controversy does not end here. Mr. Fernandes, learned Amicus Curiae would urge that it was a case for discharge but the trial court failed to appreciate the factual matrix in proper perspective. The learned Magistrate by order dated 19.2.2015 has found existence of prima facie case for the offences punishable under Section 420 IPC and Section 66-A(b) of I.T. Act, 2000 read with Section 34 IPC. It is submitted by Mr. Fernandes that Section 66-A of the I.T. Act, 2000 is not applicable. The submission

need not detain us any further, for Section 66-A of the I.T. Act, 2000 has been struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2) in Shreya Singhal v. Union of India (2015) 5 SCC 1 2015 Indlaw SC 211. The only offence, therefore, that remains is Section 420 IPC. The learned Magistrate has recorded a finding that there has been no impersonation. However, he has opined that there are some material to show that the petitioners had intention to cheat. On a perusal of the FIR, it is clear to us that the dispute is purely of a civil nature, but a maladroit effort has been made to give it a criminal colour.

29. In the present case, it can be stated with certitude that no ingredient of Section 420 IPC is remotely attracted. Even if it is a wrong, the complainant has to take recourse to civil action. The case in hand does not fall in the categories where cognizance of the offence can be taken by the court and the accused can be asked to face trial. In our considered opinion, the entire case projects a civil dispute and nothing else. Therefore, invoking the principle laid down in State of Haryana v. Bhajan Lal 1992 Supp. (1) SCC 335, we quash the proceedings initiated at the instance of the 8th respondent and set aside the order negativing the prayer for discharge of the accused persons. The prosecution initiated against the petitioners stands quashed. Consequently, the writ petition is allowed to the extent indicated above. There shall be no order as to costs. Petition allowed

---

Rajesh S/o Bhaskaran v State of Kerala

2013 Indlaw KER 1097, 2014 CRLJ 204

Bench: K. Harilal, J

The Order of the Court was as follows :

1. This Revision Petition is filed challenging the impugned order passed in CMP.No.147/2012 in CC.No.140/2010 on the files of the Judicial First Class Magistrate Court, Muvattupuzha, dismissing the above petition filed by the Revision Petitioner u/s. 239 of the Code of Criminal Procedure, seeking discharge from prosecution.

The Revision Petitioner is the sole accused in CC.No.140/2010 on the files of the Judicial First Class Magistrate Court, Muvattupuzha as well as Crime No.14/2009 in CCPS/Kerala, Thiruvananthapuram of Cyber Crime Police Station, Kerala, from which the above Calender Case had been arisen.

2. Originally he was the accused in Crime No.1499/2010 of Muvattupuzha Police Station registered for the offence punishable u/s. 66 of the Information Technology Act (for short 'IT Act') and the Crime No.399/2009 of the Vanchiyoor Police Station registered for the offence punishable u/s. 66 of the IT Act and Section 420, 379 r/w.S. 34 of the Indian Penal Code. These two crimes were registered alleging the same act alleged to have been committed by the accused. But, by the order No.D5/76776/2009 issued by the Director General of Police, the above two cases were transferred to Cyber Police Station, SCRB, Thiruvananthapuram. Now, after investigation, a final report has been filed by the Circle Inspector of Police, Cyber Police Station, Thiruvananthapuram before the Judicial First Class Magistrate Court, Muvattupuzha against the Revision Petitioner/accused alleging offence punishable u/s. 469 of the IPC alone, after deleting the offence punishable u/s. 66 of the IT Act and also all other offences alleged against the Revision Petitioner/accused for the offences punishable under the India Penal Code.

3. The prosecution case in brief is as follows: On 3.7.2009, the Revision Petitioner/the accused who is the Assistant Manager of the Zonal Office of the State Bank of Travancore (SBT, Panampilly Nagar), Ernakulam had used the E-mail address of the Muvattupuzha branch of the State Bank of Travancore and sent a message to CW6, who is the Assistant General Manager and also the Head of the Vigilance Department of SBT, Head Office, Thiruvananthapuram, stating as follows:

"Your bank is doing unduly favour to M/s.K C Wood Industries Ltd - Wood manufactures of Muvattupuzha. The project proposal submitted by us is rejected citing various reasons by your regional manager. At the same time the limit enjoyed by K C Wood Industries has enhanced from 25 Lacs to 50 Lacs. We are doing same business and the K C Wood Industries has not doing business for a limit of 50 Lacs. So it's unduly personal favour done by your regional manager. Please enquire about such proposals sanctioned and rejected from Muvattupuzha."

It is alleged that the Revision Petitioner had forged and sent an electronic record in the name of an enterprenour by name V.K.Ibrahim & Sons, which was not in existence on 3.7.2009, from the internet caffe owned by the Cw4 at Panampilly Nagar, Ernakulam. Thus, the Revision Petitioner/accused had thereby caused a loss of reputation to the Bank and Cw1 by sending the above message using the forged E-mail address and thereby committed the offence punishable u/s. 469 of Cr.PC.

4. The Revision Petitioner has filed CMP.No.147/2012, in the above case seeking discharge from prosecution mainly on the ground that Cyber Police Station, Thiruvananthapuram has no authority or power to file a final report to charge sheet him for the offence punishable under the IPC alone, when there is no police charge under the Information Technology Act in the final report. Similarly, the allegations in the charge even if admitted at its entirety, do not disclose the offence alleged against him. The learned Magistrate after hearing both parties dismissed the petition by the impugned order. This order is under challenge in this Revision Petition.

5. The learned Senior counsel for the Revision Petitioner Sri.C.C.Thomas advanced arguments based on the grounds raised in the Revision Petition. The learned Senior counsel submitted that in investigation no offence punishable under the IT Act was disclosed and the Revision Petitioner is not charge sheeted thereunder. So, the Station House Officer of the Cyber Police Station, Thiruvananthapuram has no authority or power to file final report against the Revision Petitioner for an offence punishable under the

IPC or any statute other than the IT Act. Thus, the prosecution itself against the Revision Petitioner on the basis of the final report filed by the Cyber Police Station is not maintainable. Secondly, even if the case is admitted at its entirety, the allegations against the Revision Petitioner do not disclose any offence u/s. 469 of the IPC. The disputed message which is alleged to have been sent, even if admitted, that does not disclose any kind of harm or injury to the reputation of either Cw1 or the Bank. Therefore, the court below ought to have allowed the petition and thereby discharged the Revision Petitioner from prosecution. Thirdly, the Senior counsel contended that even if the allegations are taken at its face value, the Investigating Officer failed to collect any evidence or material objects so as to prove the case against the Revision Petitioner beyond reasonable doubt. Being an offence alleged to have been committed through an electronic media, in the absence of material object by which the alleged message is said to have been sent, no offence alleging fabrication of electronic record can be proved. In short, the prosecution is only an experimental exercise intended to harass the Revision Petitioner by abusing the process of the court. The complaint was filed vindictively by another Officer of the same Bank to wreck-vengience against the Revision Petitioner without any basis.

6. Per contra, the learned Public Prosecutor advanced the argument to justify the impugned order. He submits that originally a crime was registered under the IT Act and was transferred to the Cyber Police Station for investigation. In such cases even if the investigation does not disclose the offence under IT Act, since the investigation has already been completed, the Station House Officer of the Cyber Police Station has power and authority to charge sheet the accused for the offences punishable under IPC even in the absence of any offence under the IT Act. Similarly, he straneously contended that the act allegedly done by the Revision Petitioner would constitute forgery and the contents of the message allegedly sent by the Revision Petitioner would harm the reputation of the Bank as well as the Cw1 and thereby offence u/s. 369 is attracted.

8. In view of the rival contentions, the first and formost question that arises for consideration is whether the Cyber Police Station of Kerala having jurisdiction over the entire State of Kerala, constituted to investigate any offence committed under the Information Technology Act, 2000 have power or authority to file final report charging offences under the India Penal Code or under any penal statute other than the Information Technology Act, in the absence of charge for any of the offences under the Information Technology Act, 2000 in the final report.

9. Let us have look at the general law provided under Cr.PC for investigation. S. 156 of the Cr.PC deals with the Police Officer's power to investigate cognizable case. According to this Section, any officer in charge of any Police Station may, without order of a Magistrate, investigate any cognizable case which a court having jurisdiction over a local area within the limits of such Station would have power to enquire into or try under the provisions of Chapter XIII. According to S. 177 of the Cr.PC, every offence ordinarily be enquired into and tried by a court within whose local jurisdiction it was committed. According to S. 4 of the Cr.PC, all offences under IPC shall be investigated and enquired into, tried and otherwise dealt with according to the provisions hereinafter contained in Cr.PC. But, according to sub s. 2 of Section 4, all offences under any other law shall be investigated, inquired into, tried and otherwise dealt with according to the same provisions but, subject to any enactment for the time being in force regulating the manner or place of investigating, inquiry into, trying or otherwise dealing with such offences. Thus, according to the general law, the investigation of an offence under IPC is vested with the Police Station having local jurisdiction over the area within which the offence has been committed and special procedure or power or jurisdiction can be prescribed for investigation of an offence under any special enactment for the time being in force. S. 5 saves special or local law for the time being in force or special jurisdiction or power conferred or any special form of procedure prescribed by any other law, for the time being in force.

10. Going by the GO.No.909/2004/Home dated 15.4.2004, it could be seen that the Government of Kerala under sub S. 2(s) of the Cr.PC and S. 78 of the Information Technology Act, 2000, constituted and declared Cyber Police Station known as 'Cyber Police Station Kerala' having jurisdiction over the entire State of Kerala to investigate any offence committed under the Information Technology Act, 2000. An explanatory note is also appended to this notification. Though, the explanatory note does not form a part of the notification it says that the explanatory note is intended to explain the purport of the notification. The explanation clarifies that Cyber Police Station is sanctioned in view of the upsurge in cyber crimes including the criminal intimidation on internet, Hate mail, Cyber stalking, website hacking, theft in internet hours, credit card frauds, child pornography, internet sexual harassment, internet bank frauds and

all other crimes where computers are instrumental to crime. The explanatory note further clarifies that "Cyber Police Station shall investigate any offence committed under the Information Technology Act, 2000 and this notification is intended to achieve the above object." To sum up, by the notification, investigation of the offences falling under the Information Technology Act, has been carved out from the general law applicable for investigation as provided under Cr.PC and given to Cyber Police Station, Kerala.

11. But, on an analysis of the said notification, I am of the opinion that the scope and extent of the jurisdiction and power of the 'Cyber Police Station, Kerala' constituted under the above notification is confined to and regulated by the Rule that emerges from the legal maxim "Expressio unius est exclusio alterius" ie., the express mention of one thing implies exclusion of another. The Law Lexicon explains the maxim - whenever a statute limits a thing to be done in a particular form, it necessarily includes in itself a negative viz., that the thing shall not be done otherwise. This Rule had been adopted in various judicial precedents from Taylor v. Taylor (1875) 1 Ch. D. 426 to GVK Industries Ltd. and another v. Income Tax Officer and another (2011(4) SCC 36 2011 Indlaw SC 135). This Rule adopted in Taylor v. Taylor is well recognised and is founded on sound principle. The court took the view that if a statute has conferred a power to do an act and has laid down the method in which that power has to be exercised, it necessarily prohibits the doing of the act in any other manner than which has been prescribed. This view has been adopted in Nazir Ahmed v. King Emperor (AIR 1936 PC 253(2)). In GVK Industries Ltd. and another v. Income Tax Officer and another (2011 (4) SCC 36 2011 Indlaw SC 135), the Supreme Court applied the said Rule as shown below:

"In this case it is the territory of India that is specified by the phrase "for the whole or any part of the territory of India". Expressio unius est exclusio alterius - the express mention of one thing implies the exclusion of another. In this case Parliament has been granted powers to make laws "for" a specific territory - and that is India or any part thereof, by implication, one may not read that Parliament has been granted powers to make laws "for" territories beyond India."

12. When we apply the Rule of "Expressio unius est exclusio alterius" in the instant case, it can be held that when a special notification expressly confers power and jurisdiction to investigate offences falling under a Special Statute only to a special investigating agency or to a particular Police Station, the Rule making authority is deemed to have intentionally excluded Power and Jurisdiction to investigate all other offences, falling under any Statute other than that Special Statute. To sum up: An implied exclusion of the investigation of all other offences from the purview or authority of the Cyber Police Station Kerala is inherent in the notification itself.

13. When an act is prescribed to be done in a specific way or when a power or authority is conferred to another with a direction to exercise power or authority for the performance of a specific thing or purpose, such act shall be done or performed in such a way only and such power or authority shall be exercised for the purpose for which the power has been conferred only and nothing more or nothing less than that. Going by the notification, in the light of explanatory note, I am of the opinion that obviously, the Cyber Police Station Kerala having sphere of authority over the entire State of Kerala is constituted for investigating offences coming under the Information Technology Act, 2000 only and nothing more than that. On a combined reading of notification and explanation thereunder, it is very clear that Cyber Police Station has the power to investigate offences coming under the Information Technology Act only and no other offences can be investigated by them. Necessarily, it follows that Cyber Police Station has no power or authority to file final report in the absence of any offence under the Information Technology Act in the final report. When none of the offences under Information Technology Act had been disclosed in investigation, the Station House Officer, Cyber Police Station should have sent back the case to the Police Station under which the offences under the Indian Penal Code had allegedly been committed. Therefore, I find that the final report has been filed without power or authority conferred by the notification and no prosecution can be launched on the basis of that final Report.

14. But here, indisputably no offence has been disclosed in investigation under the Information Technology Act. Consequently, the Revision Petitioner has not been charge sheeted for any of the offences under the Information Technology Act in the final report. The present final report is filed charging offence under the Indian Penal Code alone for which the Cyber Police Station has no power or authority. Whether the Cyber Police Station has power to investigate offences coming under the penal code or any other penal statute other than the Information Technology Act along with offences coming

under the Information Technology Act and to file final report charging such offences under other statutes also along with the offences under the Information Technology Act? Considering the facts of the instant case, this question does not arise for consideration and both parties did not address on that issue as it is not necessary. So, I leave it open there.

15. The decision in Prakashkumar v. State of Gujarat [2005 Indlaw SC 17] is not applicable to the instant case. Thereby interpretation of Sec.12(1) and (2) of the TADA, the Apex Court held that once the other offences under other Statutes are connected with the offence under the TADA, if the accused is charged with all the offences, the designated court is empowered to convict the accused for the offence under any law notwithstanding the fact that no offence under the TADA is made out. Here the question is entirely different. There, the S. 12(1) of the TADA empowers the designated court to try the offences under different Statutes other than the TADA along with the TADA. But here the notification does not permit so. The Cyber Police Station cannot file charge sheet under the Indian Penal Code. I have considered the decisions reported in Bhanuprasad v. State of Gujarat (AIR 1968 Supreme Court 1323 1968 Indlaw SC 45); State v. Nalini [(1999) 5 SCC 253 1999 Indlaw SC 810] and State of Tamil Nadu v. Nalini (AIR 1999 SC 2640 1999 Indlaw SC 810). But these decisions do not render any assistance to justify the lack of power involved in this case. The learned Public Prosecutor further points out that the decision in H.N. Rishbud v. State of Delhi (AIR 1955 SC 196 1954 Indlaw SC 14) a defect or illegality in investigation, however, serious, has no direct bearing on the competence or the procedure relating to cognizance or trial. I am of the opinion that the said proposition cannot be imported to the case where the Police Officer who has no power or authority, has filed a final report, which is incurable in all respects.

16. The next point for consideration is **whether there is any material documents to prove that the offence had been committed by the revision petitioner.** What is revealed in the investigation is that the message had been sent from the Internet Cafe of Cw4 on 3/7/2009, using the IP address allotted to Cw4. Admittedly on 3/7/2009, 11 persons had visited the Internet Cafe and used the facilities on hire. Since 45 days have already been elapsed, video clippings had been deleted automatically. Besides, Cw4 himself had effected formating and also wiped off several times through wiping tools. The video clippings of those who visited the Cafe as customers on 3/7/2009 are not available according to Cw4 and it cannot be decoded again as already wiped off by automatic deletion. The statement of Cw4 is supported by the statement of his employees Cw7 and Cw8 also. Thus, the crucial material object is not available in the hands of prosecution. Instead of video clippings of the customers on 3/7/09, the prosecution has seized C.Ds. containing visuals of those who visited the Cafe on 9/10/09 and 16/10/09 merely on the reason that the Revision Petitioner had visited the Cafe on those days ie., after three months. Indisputably, these C.Ds. will not serve the purpose of proving the prosecution case. I am of the opinion that the material evidence to show the person who sent the message is not available with the prosecution.

17. Similarly, the statements of Cw4 and two employees Cw7 and Cw8, show that even in the log book the number and details of each cabin which was used by each customer including the accused on 3/7/09 is not available in the log book as that column is left blank by omission. Therefore, even if the revision petitioner visited the Cafe on 3/7/09, the computer which is said to have been used by the revision petitioner is not identifiable. In the final report, it is also stated that since the video clippings containing the visuals of the persons who visited the Cafe on 3/7/09 are not available, the computer and its hard disc have not been seized and taken into custody by the police as Material Objects.

18. The last point raised by the learned Senior counsel is that the contents of the message do not cause any harm to the reputation of either Cw1 or the Bank. It is pertinent to note that the allegation is that the project proposal of one V.K. Ibrahim was rejected on various reasons. But at the same time, the credit limit enjoyed by K.C. Wood Industries has been increased from Rs.25 lakhs to Rs.50 lakhs. It is also alleged that the same is an undue personal favour done by the Regional Manager. It is to be noted that no kind of undue pecuniary benefit, ill-will, ulterior motive or mala fides had been attributed against the said Regional Manager. In short, the allegation is that the attitude shown by the Regional Manager was discriminatory or, at the most, he has violated the norms or showed some undue favour. The allegation is thus confined to an act done in discharge of the official duty and nothing more than that. More pertinently, the message was intended to make an enquiry on his complaint as obviously the same is the concluding request. I am of the opinion that the message can be depicted as a complaint and if the allegation is not true, it is only a false complaint. It is to be noted that Cw6 Job Abraham, the Asst.Manager, Vigilance Wing as well as the recipient of the message had given a statement that no independent vigilance enquiry had been conducted so far by the Vigilance Department of the State Bank

of Travancore, as he believed the statement of Branch Manager and Zonal Manager, despite the receipt of this message indicating discrimination in granting loan. I am of the opinion that the message does not disclose an intend to harm the reputation of the Bank or Cw1, the essential ingredient constituting the offence under Sec.369 Indian Penal Code; but intended for embarking an enquiry.

19. More interestingly, the Deputy Manager, State Bank of Travancore, Muvattupuzha Branch, has given a statement that K.C. Wood Industries had submitted an application for enhancing their credit limit from Rs.25 lakhs to Rs.50 lakhs and that application is being kept in the office and he is ready to produce it. No independent investigation has been made by the police to find out whether the allegations in the message are true? No such materials are available in the final charge except the statements of complainants.

20. Thus, the crucial Material Objects on which the prosecution case rests are not available, even according to the prosecution. Thus, there is no material to connect the revision petitioner with the alleged offence. So, I am of the opinion that not only the charge in the final report but also the materials produced along with the final report do not disclose the offence said to have been committed by the accused even if the uncontroverted prosecution case is admitted. Thus, there are no sufficient grounds to prosecute the revision petitioner even if the uncontroverted prosecution case is admitted. If the prosecution is allowed to continue with trial, certainly it will be a futile experimental exercise as well as abuse of the process of the Court.

21. Consequently, the impugned order under challenge passed by the court below is set aside and C.M.P.No.147/12 in C.C.No.140/10 on the files of the Judicial First Class Magistrate's Court, Muvattupuzha, will stand allowed. In the result, the revision petitioner is discharged from the prosecution for the offences alleged against him in the above Calendar Case.

Rishi Narula v State (NCT of Delhi) and others

2016 Indlaw DEL 234

The Judgment was delivered by: P. S. Teji, J.

1. The present petition under Section 482 Cr.P.C. has been filed by the petitioner, namely, Mr. Rishi Narula for quashing of FIR No.41/2014 dated 25.01.2014, under Sections 420/419 IPC & Sections 66/66C/66D Information Technology Act registered at Police Station Kirti Nagar on the basis of the compromise deed executed between the petitioner and the respondent no. 2, namely, SBI Cards Payment and Service Pvt. Ltd., Delhi through its authorized signatory-Mr. Mukesh Giri on 22.02.2014.

3. The factual matrix of this present case is that the FIR in question was lodged by the complainant on the allegation of misusing the credit cards facility of SBI Cards for unlawful gains by making unsolicited calls to SBI credit cardholders. The complainant is a registered Company. The Company checked the alleged card accounts and found that mobile number and email id was changed and new ones were updated. Later on, on enquiry it was found that the customers never requested the Company to change their mobile number and email. They also informed that they received some phone calls on behalf of SBI card agents asking for card details. The Company is alleged to have never shared customer details to any third party and never instructed any third party to make such calls. On enquiry, merchant Snapdeal informed them that a product of Sony was booked in the name of Mr. Harjit Singh and two other products are yet to be delivered. It was discovered that the said person has caused wrongful loss to the tune of Rs. 1,62,964/- to the said cardholders. Thereafter the FIR in question was lodged against the petitioner. The petitioner was in judicial custody since 25.01.2014 and was granted bail thereafter. Later on, the matter was compromised between the parties.

4. Respondent No.2 present in the Court, submitted that the dispute between the parties has been amicably resolved. As per the contents of the Compromise Deed, both the parties have settled the dispute and have agreed that the petitioner shall, prior to the filing of the petition for quashing the FIR in question, make a payment of Rs 36,951/- to respondent no.2 towards the loss suffered by the company/its customers due to the act committed by the petitioner. It is agreed that thereafter the said amount of Rs 36,951/- was paid by the uncle of the petitioner vide receipt no. 17489301 of a sum of Rs.29,820/- and receipt no. 1749302 of a sum of Rs. 5,897/- on 31.01.2014. It is further agreed that as per the instructions of respondent no.2 that the remaining amount of Rs. 1,231 has been deposited by the petitioner and duly received and acknowledged by respondent no.2 vide receipt no. 17489303 on 11.02.2014. It has also been agreed that respondent no.2 has received direct credit back from the merchants (Snapdeal/Mega deals) for an amount of Rs. 1,12,910/-. Therefore it is finally agreed between the parties that the respondent no.2 shall not object if the petitioner were to file a quashing petition. The affidavit dated 24.02.2014 of Sh. Mukesh Giri, authorized signatory/authorized representative of respondent no. 2 has been placed on record. Mr. J.P.Sundriyal affirmed the contents of the aforesaid compromise deed and of the said affidavit. In the affidavit, it is stated that respondent no.2 has no objection if the FIR in question is quashed. All the disputes and differences have been resolved through mutual consent. Now no dispute with petitioner survives and so, the proceedings arising out of the FIR in question be brought to an end. Statement of Sh. J.P. Sundriyal, authorized signatory/authorized representative of respondent No.2, has been recorded in this regard in which it is stated that the respondent no.2 has entered into a compromise with the petitioner and has settled all the disputes with him. It is further stated that respondent no.2 shall have no objection if the FIR in question is quashed.

5. In Gian Singh v. State of Punjab (2012) 10 SCC 303 2012 Indlaw SC 314 Apex Court has recognized the need of amicable resolution of disputes in cases like the instant one, by observing as under:-

"61. In other words, the High Court must consider whether it would be unfair or contrary to the interest of justice to continue with the criminal proceedings or continuation of criminal proceedings would tantamount to abuse of process of law despite settlement and compromise between the victim and the wrongdoer and whether to secure the ends of justice, it is appropriate that criminal case is put to an end and if the answer to the above question(s) is in the affirmative, the High Court shall be well within its jurisdiction to quash the criminal proceedings."

7. The inherent powers of the High Court ought to be exercised to prevent the abuse of process of law and to secure the ends of justice. The respondent no.2 agreed to the quashing of the FIR in question and has,

vide its authorized representative/ authorized signatory, stated that the matter has been settled out of its own free will. As the matter has been settled and compromised amicably, so, there would be an extraordinary delay in the process of law if the legal proceedings between the parties are carried on. So, this Court is of the considered opinion that this is a fit case to invoke the jurisdiction under Section 482 Cr.P.C. to prevent the abuse of process of law and to secure the ends of justice.

8. The incorporation of inherent power under Section 482 Cr.P.C. is meant to deal with the situation in the absence of express provision of law to secure the ends of justice such as, where the process is abused or misused; where the ends of justice cannot be secured; where the process of law is used for unjust or unlawful object; to avoid the causing of harassment to any person by using the provision of Cr.P.C. or to avoid the delay of the legal process in the delivery of justice. Whereas, the inherent power is not to be exercised to circumvent the express provisions of law.

9. It is settled law that the inherent power of the High Court under Section 482 Cr.P.C. should be used sparingly. The Hon'ble Apex Court in the case of State of Maharashtra through CBI v. Vikram Anatrai Doshi and Ors 2014 Indlaw SC 637. and in the case of Inder Singh Goswami v. State of Uttaranchal has observed that powers under Section 482 Cr.P.C. must be exercised sparingly, carefully and with great caution. Only when the Court comes to the conclusion that there would be manifest injustice or there would be abuse of the process of the Court if such power is not exercised, Court would quash the proceedings.

In the present case, the offence under Section 420 IPC is an offence compoundable with the permission of this Court as per Section 320 (2) Cr.P.C. Keeping in view, the above mentioned facts and circumstances, the offence under the said section is compounded.

11. In the facts and circumstances of this case and in view of statement made by the respondent No.2, the FIR in question warrants to be put to an end and proceedings emanating thereupon need to be quashed.

12. Accordingly, this petition is allowed and FIR No.41/2014 dated 25.01.2014, under Sections 420/419 IPC & Sections 66/66C/66D Information Technology Act registered at Police Station Kirti Nagar and the proceedings emanating therefrom are quashed against the petitioner. This petition is accordingly disposed of.

(2018) 15 Supreme Court Cases 551

(*Record of Proceedings*)

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on February 27, 2015

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on March 13, 2015

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on March 20, 2015

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 10, 2015

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on July 24, 2015

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

§ **Ed.**: Given the nature of these orders, they have been published in SCC, together, in chronological order, by the date of the order, as one combined report with the citation: (2018) 15 SCC 551. This is to facilitate a holistic view of the matters decided in such orders. Furthermore, to make it possible to search for a particular order by date as well, in SCC OnLine, each order has been reported separately with an independent citation with reference to the page on which it falls in SCC, in the combined report of all the orders i.e. (2018) 15 SCC 558; (2018) 15 SCC 560; (2018) 15 SCC 561; (2018) 15 SCC 563; (2018) 15 SCC 564 (1); (2018) 15 SCC 564 (2); (2018) 15 SCC 565 (1); (2018) 15 SCC 565 (2); (2018) 15 SCC 567; (2018) 15 SCC 569 (1); (2018) 15 SCC 569 (2); (2018) 15 SCC 569 (3); (2018) 15 SCC 570 (1); (2018) 15 SCC 570 (2); (2018) 15 SCC 571; (2018) 15 SCC 572; (2018) 15 SCC 573; (2018) 15 SCC 581; (2018) 15 SCC 582; (2018) 15 SCC 583 (1); (2018) 15 SCC 583 (2) and (2018) 15 SCC 583 (3).

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on November 21, 2016

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on December 5, 2016

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on February 1, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on March 22, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND DEEPAK GUPTA, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 5, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND DEEPAK GUPTA, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 11, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND DEEPAK GUPTA, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 13, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on May 8, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on August 22, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on September 4, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on September 18, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on October 23, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on December 11, 2017

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on January 8, 2018

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on February 15, 2018

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on March 12, 2018

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

With

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)§

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 16, 2018

PRAJWALA LETTER DATED 18-2-2015 VIDEOS OF SEXUAL VIOLENCE AND RECOMMENDATIONS, IN RE

Suo Motu WP (Crl.) No. 3 of 2015, decided on February 27, 2015

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on March 13, 2015

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on March 20, 2015

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 10, 2015

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on July 24, 2015

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on November 21, 2016

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on December 5, 2016

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on February 1, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on March 22, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 5, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 11, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 13, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on May 8, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on August 22, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on September 4, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on September 18, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on October 23, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on December 11, 2017

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on January 8, 2018

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on February 15, 2018

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on March 12, 2018

With

Suo Motu WP (Crl.) No. 3 of 2015, decided on April 16, 2018

A. **Constitution of India — Art. 21 — Distribution of sex crime videos (rape and gang rape) through social media like WhatsApp — Nationwide protest, "Shame The Rapist", by Prajwala (an organisation) exposing faces of 6 rapists urging nation to help trace them — Held, matter of great public importance — Suo motu writ petition registered on basis of letter**

of Prajwala — Prajwala further submitted 6 suggestions — Directions issued (Paras 1 to 7)

— Registry directed to keep DVDs and pen drive of said videos in sealed cover — Notice issued (Paras 8 to 11)

— CBI directed to probe all such videos, immediately register crime case and investigate (Paras 12 to 14)

— Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Distribution of sex crime videos (rape and gang rape) through social media like WhatsApp

B. **Constitution of India — Art. 21 — Distribution of sex crime videos (rape and gang rape) through social media like WhatsApp — Judicial notice taken of steps taken on 13-3-2015 and 20-3-2015 — Directions issued with regard to identification and arrest of culprits, and transfer of RCs to CBI, recording of statements of victims, further investigation by CBI under S. 173(8) CrPC and blocking of sites — CBI directed to ascertain persons who uploaded clips in social media**

— Matter already referred to Computer Emergency Response Team, India and steps taken to nominate Nodal Officers — Google requested for assisting identification of said persons (Paras 15 to 31)

C. **Constitution of India — Art. 21 — Distribution of sex crime videos (rape and gang rape) through social media like WhatsApp — Costs of Rs 50,000 and Rs 25,000 imposed on States of Odisha and Telangana for non-appearance in such important matter and not seriously taking steps regarding attack on vehicle respectively — Personal appearance of Chief Secretary, Odisha, directed — Resultantly both States taking effect steps (Paras 18, 19 and 32 to 39)**

D. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Effective tackling of cyber crime — Suggestions of Committee formed by Central Government — 2 suggested schemes approved by Government — Directions issued to update court on all such schemes — Matter adjourned (Paras 42 to 48)**

E. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Child pornography (CP), rape/gang rape (RGR) videos — Notice issued and parties impleaded (Paras 49 to 51, 59, 68 and 69)**

F. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Child pornography (CP), rape/gang rape (RGR) videos — Cyber Crime Prevention against Women and Children (CCPWC) as Central Institutional Mechanism — Constitution, duties, functions, infrastructure and setting up of — Directions — Needful should be done within two weeks (Paras 52 to 55)**

G. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Child pornography (CP), rape/gang rape (RGR) videos — Steps not to make said videos available to general public — Feasibility — Committee to advise on feasibility formed with stated constitution — Meeting of committee for said purpose — Accordingly directed — Directions issued**

with regard to confidentiality and action/prosecution in respect of complaints received (Paras 63, 64 and 71 to 93)

H. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Child pornography (CP), rape/gang rape (RGR) videos — Committee to advise on feasibility of restricting said videos to general public — Temporary substitution of Chairperson of Committee permitted due to ill health of functioning Chairperson (Paras 66 and 67)**

I. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Child pornography (CP), rape/gang rape (RGR) videos — Recommendations of Committee on feasibility of restricting said videos to general public — Parties including Government directed to abide by recommendations on which there is consensus — Confidentiality with regard to technology used for purpose directed to be kept confidential — Government directed file status report on next date — Facebook directed to give progress status of Artificial Intelligence (AI) based new proactive technology — Administrative proposals be separated form technological proposals (Paras 94 to 122)**

J. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Child pornography (CP), rape/gang rape (RGR) videos — Steps not to make said videos available to general public — Complaint portal for reporting such issues — Central Government directed to have portal ready by 10-1-2018 and file progress report by 8-1-2018 — It is high time that said portal is made available to public (Paras 109 to 128)**

K. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Child pornography (CP), rape/gang rape (RGR) videos — Steps not to make said videos available to general public — Identification of search keywords for cyber surveillance — Government identifying English language keywords for CP and RGR content search — Task for such keywords identification for other languages to be taken up soon (Para 113)**

L. **Information Technology, Internet, Computer and Cyber Laws — Cyber Crimes — Child pornography (CP), rape/gang rape (RGR) videos — Steps not to make said videos available to general public — Central Reporting Mechanism — Held, it would be in interest of all if Central Reporting Mechanism is set up — Home Ministry directed to file detail status/progress report keeping in view roadmap prepared — Status report should deal with all issues comprehensively (Paras 129 to 134)**

SS-D/60320/SR

Advocates who appeared in this case :

Surya Prasad Mishra, Attorney General, Maninder Singh, Neeraj Kishan Kaul, Additional Solicitors General, Vijay Bahadur Singh, Advocate General, V.K. Shukla, Vijay Shukla, Vijay K. Shukla, Additional Advocates General, L. Nageswara Rao, Jayesh Gaurav, Huzefa Ahmadi, Arvind Verma, Sidharth Luthra, V. Giri, Dr A.M. Singhvi, Kapil Sibal and Sajan Poovayya, Senior Advocates [Ms Aparna Bhat, S.A. Haseeb, Ms Gunwant Dara, Ajay Sharma, R. Balasubramanian, Santosh Kumar, T.A. Khan, Ms Sushma Suri, D.S. Mahra, B.V. Balaram Das, Gopal Prasad, B. Balaji, R. Rakeshsharma, Ms R. Shase, Ravi Prakash Mehrotra, Vibhu Tiwari, Kabir Shankar Bose, Anip Sachthey, P. Ramesh Kumar, Ms Tanima Kishore, B.V. Balaram Das (Advocate-on-Record) Ms Atreyi Chatterjee, P. Venkat Reddy, Sumanth Nookala (for M/s Venkat Palwai Law Associates), Ravi Prakash Mehrotra (Advocate-on-Record),

Anip Sachthey (Advocate-on-Record), Sumit Kumar, Ms Shivangi Singh, S.N. Terdal, P. Venkat Reddy (for M/s Venkat Palwai Law Associates), Saakaar Sardana, Shibashish Mishra (Advocate-on-Record), Ranjan Mukherjee, Ms Sunitha Krishnan (for Prajwala), Ms Suman Suri, Kabir S. Bose, Ms Shagun Matta, Gopal Prasad, Pukhrambam Ramesh Kumar, Raj Kumari Banju, Mayank Sapra, R. Bala, P.K. Dey, B.K. Prasad, Mukesh Kr. Maroria, Jayesh Gaurav, Parijat Sinha, Gajendra Parsad Singh, Shibashish Misra, Prabhas Bajaj, Ms Sushma Suri (Advocate-on-Record), B. Krishna Prasad, Mukesh Kr. Maroria (Advocate-on-Record), Debjyoti Basu, Parijat Sinha (Advocate-on-Record), Ashish Kr. Sinha, Sankara Kaushik, Gopal Prasad (Advocate-on-Record), Ms N.S. Nappinai (Amicus Curiae), Ananya Mishra, Ms Reshmi Rea Sinha, Rudra Dutta, Sankara Kaushik, Sanjay Singh, Sohan, S. Alam, Samir Ali Khan (Advocate-on-Record), Akhil Anand, Ms Richa Srivastava, S.S. Shroff (Advocate-on-Record), Ms Ruby Singh Ahuja, Vishal Gehrana, Ms Tahira Karanjawala, Arvind Chari, Ms Manik Karanjawala (for M/s Karanjawala & Co.), Amar Gupta, Divyam Agarwal, Ms N.S. Nappinai (Amicus Curiae) (Advocate-on-Record), Ms Aparna Bhat (Advocate-on-Record), Tejas Karia, Nitin Saluja, Akhil Bhardwaj, Ms Divyam Agarwal (Advocate-on-Record), R.N. Karanjawala, Aavishkar Singhvi, Ms Suman Yadav, Priyadarshi Banerjee, Ms Rashmi Malhotra, V.B. Chaurasia, Syed Abdul Haseeb, Umesh Babu Chaurasia, R.R. Rajesh, Raj Bahadur Yadav, Shibashish Misra (Advocate-on-Record), R. Bala (Mentioned by), Ms Joshita Pai, Rohit Rathi, Ms Nandini Sen, Chanchal Kr. Ganduli, Sanjay Kumar, Soham Kumar, Arpit Gupta, Kushank Sindhu, Vivek Reddy, Shashank Mishra, Akshay Amritanshu, G. Dera, Utkarsh Sharma, C.K. Ganguli, Ms K. Enatoli Sema, Edward Belho, Amit Kr. Singh, K. Luikang Michael, Ms Elix Gangmei, Z.H. Issac Haiding, Ms Saanjh N. Purohit, Pranav Avasthi, Arpit Gupta, Koshy John, Raghav, Kartikey Bhargava, Aman Sinha, Aarti Sharma, Rajeev Kr. Dubey, Vinay Garg, Ms Nandini Sen, Chanchal Kr. Ganguli (Advocate-on-Record), Ms Saanjh Purohit, Ginni Sehgal, Kumar Vaibhav, Pranav Awasthi, Shravan Sahny, Ashwin Reddy, Ms Shushma Suri (Advocate-on-Record) (Not Present), Saransh Kumar, Sharvan Sahny, Avishkar Singhvi (for M/s Karanjawala & Co.), S.S. Shroff (Advocate-on-Record) (Not Present), Anupam Prakash, Pratibha Kharola, Mukesh Kr. Maroria (Advocate-on-Record) (Not Present), Ms Raj Kumari Banju, Manu Krishnan, S. Pratibhanu Singh Kharela, Rahat Sharma, S. Partibhanu Singh Kharola, Shijo George, Ms Ishani Banerjee, Ms Trishala Kulkarni, Raghav Tankha, Aman Singh, Mrinal Srivastava, Kuber Dewan, S.S. Shroff, Advocates] for the appearing parties.

(2018) 15 SCC 558

ORDER dated 27-2-2015

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

1. A letter dated 18-2-2015 was addressed to Hon'ble the Chief Justice of India by Prajwala, an organisation based in the old city of Hyderabad. The letter was handed over to one of us by the office of Hon'ble the Chief Justice of India. On reading the letter, it is quite clear that an issue of great public importance has been raised. Accordingly, suo motu petition has been registered based on the contents of the letter.

2. Ms Aparna Bhat, learned counsel appears on behalf of Prajwala and she submits that she will file a detailed petition giving suggestions with regard to the issues raised in the letter.

3. The letter states that the General Secretary of Prajwala came to learn of two videos, one of which is 4.5 minutes long wherein one man is raping a girl and another is recording the incident. This incident appears to have occurred

somewhere in Delhi-Uttar Pradesh. The second video is about 8.5 minutes long and is of a gang rape wherein five men were seen raping a very young woman. The second video is from some "Bengali like speaking region". It is further stated in the letter that apart from the fact that the incidents of rape and gang rape were video recorded, to make matters worse, they have been distributed through WhatsApp.

4. When Prajwala learnt of the videos, a nationwide campaign Shame The Rapist was launched on 5-2-2015 exposing the faces of the rapists (1 + 5) and requesting the nation to help trace the culprits. It is stated that the campaign has gone viral with thousands of people joining the campaign and one of the results of the campaign was that it has come to notice that there are certain websites which cater only to pornographic videos of sexual violence. These websites have been mentioned in the letter sent by Prajwala.

5. In the opinion of Prajwala, the incidents indicate that the offence of rape is committed with impunity and the offender even has the audacity to flaunt the incident in the public domain through a video recording. This has a negative impact on the criminal justice system and also makes it difficult for the common people to report such matters to law enforcement agencies.

6. Prajwala has made six suggestions in the letter. These are:

(*i*) A CBI probe into all such videos with the findings being made public;

(*ii*) Setting up of a Task Force on Sexual Crimes. The Task Force should be set up within the Ministry of Home Affairs and should also focus on technology driven sexual crimes.

(*iii*) A public friendly mechanism to report such videos. It is suggested that a mechanism could be evolved to have a secure email Id and also a toll free number which will enable citizens to report such crimes without any threat perception.

(*iv*) A National Sex Offenders Register of convicted sex offenders. This will be more in the nature of a Registry which will give publicity to the sex offenders which could include those indulging in eve-teasing, molesters, stalkers and rapists and other similar offenders.

(*v*) Tie-up of the Ministry of Home Affairs with YouTube and WhatsApp so that dissemination of offensive videos and material relating to sexual crimes is curbed and penal action taken against the offenders.

(*vi*) Specialised training of senior law enforcers on issues relating to sexual crimes and cyber space and other use of technology to tackle concerns from social media and other technology enabled applications such as WhatsApp and YouTube.

Attached with the letter is a pen drive with videos received by Prajwala and DVDs of the videos. The Registry should keep the pen drive and DVDs in a sealed cover.

7. On the basis of the contents of the letter, it is quite clear that the issues raised are extremely serious and are of great public concern.

8. Under the circumstances, we issue notice to the States of Uttar Pradesh, West Bengal, Odisha and the NCT of Delhi. The notice may be served through the Chief Secretary of the States and the NCT of Delhi and also through the Director General of Police in the States and the Commissioner of Police in Delhi.

9. The Government of India, through the Secretary, Ministry of Home Affairs and the Secretary, Ministry of Communications and Information Technology are necessary parties, particularly in view of the suggestions that have been made in the letter. Accordingly, notice may also be issued to the Government of India, through the Secretary, Ministry of Home Affairs and the Secretary, Ministry of Communications and Information Technology.

10. We have been informed by the learned counsel that subsequent to the social media campaign ShameTheRapist, the vehicle of the General Secretary of Prajwala was attacked in Hyderabad (Telangana). It is also, therefore, necessary to issue notice to the Chief Secretary and the Director General of Police in the State of Telangana.

11. We have also been informed by Ms Aparna Bhat that no significant progress seems to have been made in apprehending the rapists or those who attacked the vehicle of the General Secretary of Prajwala. We expect the police forces in the States concerned and NCT of Delhi to take urgent and immediate action to identify and apprehend the culprits.

12. Since the first suggestion made by Prajwala is for a CBI probe into all such videos, notice may also be issued to the Director, CBI to immediately register a crime and to start investigations with immediate effect. Ms Aparna Bhat states that she will, if possible, make additional copies of the pen drive and DVDs and supply them directly to the Director of CBI. She further states that in case she is not able to do so, the pen drive and DVDs copies of which are already available with the Secretary in the Ministry of Home Affairs, Government of India may be transmitted by the Secretary in the Ministry of Home Affairs to the Director, CBI for necessary action and to commence investigations or collected by the Investigating Officer from the said Secretary. Given the seriousness of the issues raised, we expect all authorities/officials to effectively cooperate with one another.

13. Ms Aparna Bhat submits that she will file the detailed petition on 9-3-2015.

14. List the matter on 13-3-2015.

(2018) 15 SCC 560

ORDER dated 13-3-2015

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

15. We have heard Mr Maninder Singh, learned Additional Solicitor General. We have requested the learned Additional Solicitor General to inform us on the next date of hearing about the steps taken by the Ministry of Home Affairs between 10-2-2015 when the email giving information about the culprits and the DVDs and pen drive along with a detailed letter was given to the Ministry of Home Affairs by Prajwala and when they were handed over to

CBI along with a covering letter on 5-3-2015. We would like to know why it took such a long time for the Ministry to react to the information supplied by the petitioner.

16. We have been told by the learned Additional Solicitor General that after receipt of the DVD and the pen drive by CBI, it was sent to the Forensic Science Laboratory to check the authenticity of the recording. A report has been received from the Forensic Science Laboratory and now a request has been made to give clear pictures of the culprits involved in the crime. It is stated that as soon as clear pictures of the culprits are made available, they will be shared with the Director General of Police in Uttar Pradesh, Odisha and West Bengal (and other States if necessary) for publication so that whoever has any information about the culprits can pass it on to CBI or the authorities concerned for the purpose of their identification. Similar steps will also be taken with regard to the Commissioner of Police in Delhi. We would expect the Director General of Police in Uttar Pradesh, Odisha and West Bengal as also the Commissioner of Police in Delhi to cooperate and coordinate efforts with CBI. Publication may be made in such of the States where CBI expects the culprits to be found.

17. In the meanwhile, CBI should also inform us on the next date of hearing about the progress made to ascertain who uploaded the clips on the internet and the investigative steps taken in this regard. The status report may be filed well before the next date of hearing.

18. We must express our anguish that in spite of service, there is no appearance on behalf of the State of Odisha despite the fact that the case is of considerable importance. Due to non-appearance on behalf of the State of Odisha, we impose costs of Rs 50,000 to be paid by the State of Odisha to the petitioner within one week from today.

19. The vehicle of the General Secretary of the Prajwala was damaged in Hyderabad (Telangana). We are told that the police in Telangana is looking into the matter and that a crime has been registered, but absolutely no particulars are made available to this Court. Accordingly, in view of the fact that the police authorities in Telangana are also taking the matter very casually, we impose # cost of Rs 25,000 to be paid by the State of Telangana to the petitioner within one week from today.

20. We have been told by the learned Additional Solicitor General that CBI has already registered eight regular cases and one preliminary enquiry and investigations are in progress. List the matter on 20-3-2015.

(2018) 15 SCC 561

ORDER dated 20-3-2015

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

21. Pursuant to our order dated 13-3-2015[1], CBI has filed a status report in a sealed cover which we have received in Court today and have gone through

1 Set out in paras 15 to 20, above.

the contents thereof. From the status report, it is quite clear that in fact 12 video clips were received out of which three of them were repetitive. Effectively, nine video clips were received by CBI. CBI has since registered eight regular cases and one preliminary enquiry on 12-3-2015.

22. With regard to six regular cases registered by CBI, investigations are going on and the photographs of the culprits have already been shared/being shared with the Director General of Police of all the States, the National Crime Records Bureau, the State Crime Records Bureau, CBI Home Page, Doordarshan and National/Regional dailies. Apart from this, CBI has also announced a reward of Rs 1,00,000 for providing information leading to the identification/apprehension of each suspect.

23. It is further stated in the status report that with regard to RC No. 7, the suspects have been identified by the State police and an FIR was registered by the State police. The suspects were arrested and were subsequently granted bail. We direct transfer of this case being Crime/FIR No. 323 of 2015 registered in Sadar Police Station, Sitapur for further investigations to CBI.

24. Mr Ravi Prakash Mehrotra, learned counsel appearing for the State of Uttar Pradesh has no objection in transfer of this case to CBI. He further states that the State police will extend all necessary cooperation to CBI in the investigations.

25. It is submitted by the learned Additional Solicitor General that about three months' time is required to complete the investigations in this case. We make it clear that CBI is entitled to carry out any further investigations and to file a report under Section 173(8) of the Code of Criminal Procedure, 1973.

26. As regards, RC No. 6, it is stated that the possible suspects have been identified and necessary steps are being taken to apprehend them. With regard to the preliminary enquiry, it is stated that the offence appears to have been committed outside India and the accused has perhaps been sentenced to imprisonment. Steps are being taken by CBI to confirm this.

27. It is submitted by the learned counsel for the petitioner that the petitioner's statement has not yet been recorded in the matter. The learned Additional Solicitor General has taken note of this submission and will discuss the matter further with the investigating officer in CBI. It is also submitted by the learned counsel for the petitioner that once the victims have been identified, their statements may be recorded with the assistance of the qualified social workers or counsellors, as the case may be, and/or medical professionals.

28. The learned Additional Solicitor General has also taken note of this and will pass on this submission to the investigating officer in CBI who will take necessary steps in this regard, as advised.

29. It is also brought to our notice that on the question of identifying the person or persons who have uploaded the video clips, the matter has been referred to the Computer Emergency Response Team — India and necessary steps are being taken to nominate a nodal officer in this regard. "Google" has also been requested to assist in the identification of the persons who have uploaded the video clips.

30. It is submitted that some sites have already been blocked at the instance of the Ministry of Home Affairs, Government of India. The learned Additional Solicitor General submits that a detailed affidavit will be filed in this regard within one week.

31. Insofar as the investigations by CBI are concerned, three months' time is granted to them to carry out the investigations. However, a status report should be filed after four weeks.

32. As far as the State of Telangana is concerned, the affidavit has been filed by the Assistant Commissioner of Police. We have gone through the affidavit filed by the Assistant Commissioner of Police and it appears that immediate steps were taken as soon as the complaints were received from the petitioner. We are satisfied with the investigations that have been made by the local police although the learned counsel for the petitioner submits that no progress has been made in the investigation.

33. Mr Neeraj Kishan Kaul, learned Additional Solicitor General submits that investigations are still in progress. It may take some time to complete the investigations. Looking to the steps already taken by the police and the State of Telangana, the costs awarded by this Court by the order dated 13-3-2015[1] are waived. On the next date of hearing, the State of Telangana will also inform us about the progress made in the investigations.

34. In spite of our earlier order dated 13-3-2015[1], there is still no one present on behalf of the State of Odisha. Costs have also not been deposited. We cannot appreciate this total lack of concern by the State of Odisha. Accordingly, we direct the presence of the Chief Secretary of the State of Odisha on the next date of hearing.

35. List the matter on 10-4-2015. The Registry should send a copy of this order to the Chief Secretary of the State of Odisha and the Standing Counsel for the State of Odisha forthwith.

(2018) 15 SCC 563

ORDER dated 10-4-2015

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

36. The Chief Secretary of the State of Odisha is present in the Court today. Mr L. Nageswara Rao, learned Senior Counsel appearing on behalf of the State of Odisha has advised the Chief Secretary to take certain remedial steps. No further orders are required to be passed in this regard. Further appearance of the Chief Secretary is dispensed with.

37. The Ministry of Home Affairs has filed an incomplete affidavit. Mr Maninder Singh, learned ASG appearing on behalf of the Ministry seeks leave to withdraw the affidavit and file an appropriate affidavit. Leave and liberty granted.

1 Set out in paras 15 to 20, above.

38. The State of Telangana has filed its affidavit. It appears that investigations are in progress and the State Police is taking up the matter with due seriousness. Under the circumstances, insofar as the investigations into the attack on the vehicle of the General Secretary of the petitioner organisation is concerned, no further directions are required to be given to the State of Telangana and they are accordingly discharged insofar as this is concerned. However, the investigations should continue.

39. List the matter on 24-7-2015.

(2018) 15 SCC 564 (1)

ORDER dated 24-7-2015

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

40. Ms Sunitha Krishnan appearing on behalf of PRAJWALA says that she has gone through the affidavit filed on behalf of the Ministry of Home Affairs and she would like to file some suggestions. She may do so in the form of a Note.

41. List the matter on 28-8-2015.

(2018) 15 SCC 564 (2)

ORDER dated 21-11-2016

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

42. The learned counsel for the petitioner has drawn our attention to an affidavit filed by CBI/Respondent 8 on 8-10-2015. She submits that CBI has some very valuable suggestions which need to be considered and appropriate orders passed thereon.

43. Our attention has also been drawn to the order dated 4-12-2015. The learned counsel for the Union of India submits that pursuant to the order dated 4-12-2015, an affidavit sworn by Mr Vedantam Giri, Joint Secretary, Ministry of Home Affairs was filed on 4-12-2015.

44. We have gone through the affidavit filed on behalf of the Ministry of Home Affairs and find that a Committee was set up by the Ministry of Home Affairs to look into the issues relating to cyber crimes and suggest a road map for effectively tackling cyber crimes in the country and giving suitable recommendations on all facets of cyber crime.

45. The Committee submitted its report in the first week of September 2015. The Ministry of Home Affairs accepted the recommendations of the Expert Committee in principle on 17-9-2015 and in principle approval has also been granted by senior officers of the Ministry of Home Affairs for two schemes viz. (*i*) Scheme for setting up Indian Cyber Crime Coordination Centre (I4C) with the estimate cost of Rs 464.28 crores (from the allocated budget of MHA). (*ii*) Scheme for setting up Cyber Crime Prevention against Women and Children (CCPWC) Unit with the estimated cost of Rs 244.32 crores (from Nirbhaya fund).

46. It is also stated in the affidavit that the data based on the Crime and Criminal Tracking Network System (CCTNS) has in principle been approved for publishing in National Sex Offenders List. A detailed concept note has been prepared in this regard and shared with the Members concerned. A module for the same has also been finalised under the Central Citizen Portal in CCTNS Project. It is further stated that setting up of the Investigative Units For Crime Against Women (IUCAW) are additional reinforcement to strengthen the existing infrastructure for tackling heinous crimes against women and in lieu of a Central Coordinating Mechanism.

47. The learned counsel should update us on the schemes along with a copy thereof with the final decision taken on publishing a National Sex Offenders List as well as the progress with regard to the Investigative Units For Crime Against Women (IUCAW).

48. List the matter on 28-11-2016 at 2.00 p.m. We make it clear that no adjournment will be granted in this regard.

(2018) 15 SCC 565 (1)
ORDER dated 5-12-2016

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

49. We have heard the learned counsel for the parties and they are at ad idem on the suggestions given by the learned counsel for the petitioner as well as by CBI and the Union of India.

50. However, before we finalise the order, it is necessary to issue notice to (*i*) Microsoft Corporation (I) Pvt. Ltd., Microsoft India Headquarters, DLF Infinity Towers 7th Floor, Tower 'B' DLF Cyber City, Sector 25A, Phase II, Gurgaon — 122002, (*ii*) Google India Pvt. Ltd., No. 3, RMZ Infinity — Tower E, Old Madras Road, 3rd, 4th and 5th Floors, Bangalore — 560 016, (*iii*) Yahoo! India Pvt. Ltd., Building 12, Solitaire Corporation Park, Guru Hargovindji Marg, Andheri (East), Mumbai — 400 093 and (*iv*) Facebook, Facebook India Headquarters, Level 12, Building No. 14, Raheja Mindspace, Hi Tech City, Vittal Rao Nagar, Hyderabad — 500 081 (Andhra Pradesh). Accordingly, notice be issued to these entities returnable on 9-1-2017.

51. List the matter on 9-1-2017 at 2.00 p.m.

(2018) 15 SCC 565 (2)
ORDER dated 1-2-2017

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

52. We have heard the learned counsel for the parties. We have also heard Ms N.S. Nappinai, learned counsel and we request her to assist us in the matter on subsequent hearings.

53. Two suggestions have been placed for consideration. The first suggestion made by the learned counsel for the petitioner is that some sort of

Central Institution Mechanism should be established by the Government of India. This suggestion seems to have the approval of the Ministry of Home Affairs, Government of India as well as the Central Bureau of Investigation (CBI). It appears that the Government of India has given in principle approval to a body called the Cyber Crime Prevention Against Women and Children (CCPWC) and the budget for the CCPWC has been approved by the Standing Finance Committee (SFC) for implementation at a cost of Rs 195.83 crores during the next three financial years. The constitution of CCPWC, its duties and responsibilities have not been mentioned in the affidavit filed on behalf of the Ministry of Home Affairs nor are the details of this body available in the affidavit filed by CBI. The learned counsel for the petitioner has suggested that this body which may also be described as a Central Institution Mechanism may address cases relating to preparation, transmission and circulation of videos depicting rape/gang rape as also videos of sexual violence of unknown women and children in the electronic media.

54. The further submission made by the learned counsel for the petitioner is that the Central Institution Mechanism may function out of a Central Cell within CBI and may be headed by an officer not lower than the rank of the Inspector General of Police. Necessary infrastructure should also be provided to this Central Institution Mechanism. We have already referred to the budget that is proposed to be made available to the Central Institution Mechanism. The learned counsel for the petitioner also says that the Central Institution Mechanism may take cognizance of cases suo motu or on the basis of a complaint made by an aggrieved person.

55. The learned Additional Solicitor General says that he will take instructions and get back to us with regard to the constitution, duties and responsibilities of the Central Institution Mechanism or CCPWC including whether it should be established in the Ministry of Home Affairs or in the office of the CBI and with regard to the necessary infrastructure, personnel and manpower for the Central Institution Mechanism or CCPWC. The needful be done within two weeks.

56. Ms Nappinai has indicated and submitted that in some western countries instead of blocking objectionable videos, uploading of videos is blocked at the first instance and thereafter the person who wants to upload the video informs the service provider that the video is copyrightable or he holds a copyright on the video and then the service provider uploads that video. This eliminates the uploading of objectionable videos. She submits that a similar sort of mechanism can be adopted for the purposes of blocking explicit videos and photographs and contents (textual contents) of objectionable material.

57. It is submitted by the learned counsel appearing for Facebook Ireland that there is already a mechanism in operation through which it is possible to scan objectionable photographs and to block them and to stop them from being uploaded. He, however, points out that there is a possibility of masking

of photographs and that may result in some objectionable photographs being uploaded. He says that he is not aware whether any such technology exists with regard to videos and he would like to take instructions in this regard.

58. The learned counsel appearing for Yahoo India, Google India and Microsoft India also say that they would like to take instructions in this regard and get back on the technological aspect and the feasibility of adopting or adapting the suggestions given by Ms Nappinai.

59. On the request of the learned counsel for Google India, Google Inc., 1600, Amphitheatre Parkway, Mountain View, CA 94043, USA (email: Support-in@google.com) is impleaded as respondent and formal notice may be issued to it. The learned counsel for the petitioner says that she will serve Google Inc. by email.

60. Any affidavit that may be filed by any of the parties should be filed within two weeks from today. List the matter on 21-2-2017 at 3.00 p.m.

(2018) 15 SCC 567

ORDER dated 22-3-2017

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

61. We have heard the learned counsel for the parties and we are glad to note that all the learned counsel are in agreement that some sort of a Committee should be constituted to assist and advise this Court on the feasibility of ensuring that videos depicting gang rape, child pornography and rape should not be made available to the general public, apart from anything else, to protect the identity and reputation of the victims and also because a circulation of such videos cannot be in public interest at all. None of the learned counsel and their clients are taking this as an adversarial litigation and they welcome the idea of setting up a Committee for this purpose.

62. The Government of India has suggested that the Committee should consist of the following persons:

1. Dr Ajay Kumar, Additional Secretary, Ministry of Electronics and Information Technology who will be the Chairman of the Group/Committee.

2. Dr Sanjay Bahl, Director General (CERT-In), Ministry of Electronics and Information Technology.

3. Mr Rakesh Maheshwari, Scientist-G, Ministry of Electronics and Information Technology.

4. Two member representatives to be detailed by the Ministry of Home Affairs who will be identified and will be present throughout the discussions.

5. Ms Aparna Bhatt, learned counsel for the petitioner.

6. Ms N.S. Nappinai, learned Amicus Curiae.

7. Mr Sidharth Luthra, learned Senior Counsel on behalf of Facebook (Ireland) has stated that the following persons will represent that entity in the Group/Committee:

(*a*) Vikram Langeh, Manager Trust and Safety South & Central Asia

(*b*) One technically qualified person to be nominated by Facebook within two days.

8. Google Inc & Google India have nominated the following persons:

(*a*) Tech: Anthony Surleraux

(*b*) Policy: Kseniia Duxfield-Karyakina

(*c*) Legal: Gitanjli Duggal (Resident of India)

9. Yahoo India has nominated the following person:

(*a*) Robin Fernandez, Grievance Officer (Resident of India)

10. Microsoft has nominated the following persons:

(*a*) Mr S. Chandrasekhar, Group Director, Govt. Affairs (Resident of India)

(*b*) Mr Radhakrishnan Srikanth, Principal Group Program Manager (Resident of India)

(*c*) Mr Balakrishnan Santhanam, Sr. Program Manager (Resident of India)

Mr V. Giri, learned Senior Counsel on behalf of Microsoft says that two of the three participants will be available in every meeting/discussion.

63. The Committee will meet on 5-4-2017 at 10.30 a.m. at the venue to be decided by Dr Ajay Kumar, Additional Secretary and communicated by him to all the participants through e-mail. We expect the Committee to hold day-to-day discussions/meetings and preferably to arrive at a consensus on the possibility of ensuring that such objectionable videos pertaining to child pornography, gang rape and rape are not made available on the internet. For some technical reasons, if this is not possible, to explain and detail the reasons why it is not possible. The results of the meetings will be kept confidential and the report will be kept in a sealed cover till it is presented to this Court.

64. The learned counsel for the parties have assured us that all the participants will be available for all the discussions and meetings in Delhi except in the event of an urgency which should be explained to Dr Ajay Kumar, Additional Secretary. We make it clear that in case any technical inputs are required by any of the parties, video conferencing facilities will be made available. Wherever visas are required to be obtained, we request the Government of India to assist in obtaining them.

65. List the matter on 24-4-2017 at 2.00 p.m. as a part heard matter.

(2018) 15 SCC 569 (1)

ORDER dated 5-4-2017

(BEFORE MADAN B. LOKUR AND DEEPAK GUPTA, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

66. Upon being mentioned, the matter is taken up. It is pointed out by the learned counsel appearing on behalf of the Union of India that Dr Ajay Kumar, Additional Secretary, Ministry of Electronics and Information Technology who, it was suggested will Chair the meeting of the Committee as mentioned in the order dated 22-3-2017[2], has fallen ill with typhoid. He says that under these circumstances it may be more appropriate if the meeting is Chaired by Arvind Kumar, Scientist G. and Group Coordinator, Cyber Laws, Ministry of Electronics and Information Technology.

67. We accede to the request made by the learned counsel. Hopefully, Dr Ajay Kumar will recover quickly. When he recovers, he may begin Chairing the subsequent meetings.

(2018) 15 SCC 569 (2)

ORDER dated 11-4-2017

(BEFORE MADAN B. LOKUR AND DEEPAK GUPTA, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

68. The matter is taken on board. On an oral request made by Ms Aparna Bhat, learned counsel for the petitioner, WhatsApp Inc. having office at 1601, Willow Road, Menlo Park, California — 94025, United States of America [Email id: WhatsappLEC@subpoenasolutions.com] is made a party respondent.

69. Since the meetings pursuant to our earlier orders are being held on day-to-day basis, issue notice to WhatsApp Inc. returnable on 13-4-2017. Dasti, in addition. In the meanwhile, the learned counsel for the petitioner may also send a detailed e-mail to the newly added respondent to make a presentation, if possible through video conferencing, to assist the Committee.

(2018) 15 SCC 569 (3)

ORDER dated 13-4-2017

(BEFORE MADAN B. LOKUR AND DEEPAK GUPTA, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

70. Mr Kapil Sibal, learned Senior Counsel appearing on behalf of Whatsapp Inc. says that Whatsapp Inc. is willing to assist and is also prepared to attend the meetings being held. In fact, he says that the following three officials of Whatsapp Inc. will participate in the meeting:

1. Matt Jones, Software Engineer
2. Keyla Maggessy, Law Enforcement Response Manager
3. Christian Dowell, Associate General Counsel

2 Set out in paras 61 to 65, above.

The learned Senior Counsel says that the representatives of Whatsapp Inc. will assist the Committee in a special meeting to be held on 27-4-2017. The non-Indian members need not stay back for that meeting since they have other commitments.

71. It is made clear that the meetings of the Committee are being held in confidence and are completely confidential and are being held under the orders of this Court.

(2018) 15 SCC 570 (1)

ORDER dated 8-5-2017

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

72. We have heard the learned Additional Solicitor General instructed by Mr Ajay Kumar who is the in-charge of the Committee set up in terms of order dated 22-3-2017[2]. A report has been filed in a sealed cover which may be taken on record and should be kept by the Registry in a sealed cover.

73. It is submitted that there are certain issues on which a final decision could not be taken and further period of four weeks is required to take a decision on these issues and to make a final and comprehensive report. In view of the above, we adjourn the matter to 6-7-2017 at 3.00 p.m. by which date we expect a final and comprehensive report to be made available. The representative of WhatsApp may be co-opted as a member of the Committee.

74. It has been pointed out by the learned counsel for the petitioner that the learned Amicus has to travel from Mumbai to attend the meetings of the Committee. To take care of her travel expenses that she is incurring from time to time, the Union of India should make a deposit of Rs 2,00,000 in the Registry of this Court which may then be handed over to the learned Amicus. The deposit be made within two weeks from today.

75. We request the Chairman of the Committee to continue to Chair the Committee till a final and comprehensive report is prepared and filed.

(2018) 15 SCC 570 (2)

ORDER dated 22-8-2017

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

76. In respect of the Report that has been submitted, we have requested Mr Ajay Kumar, the Chairman of the Committee and the learned counsel for the parties to take instructions from the participants whether they have any objection to the Report being placed in the public domain with regard to the contents as well as the recommendations made for which there is unanimity and the recommendations for which there is no unanimity.

2 Set out in paras 61 to 65, above.

77. List the matter on 4-9-2017 at 2.00 p.m.

(2018) 15 SCC 571

ORDER dated 4-9-2017

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

78. We have heard the learned Amicus Curiae as well as the learned counsel for the parties and Mr Ajay Kumar, Chairperson of the Committee appointed by this Court.

79. It has been brought to our notice by Mr Ajay Kumar that the entities that had participated in the meetings have tentatively objected to the report being placed in the public domain but they would like to take a final decision in this regard. In our opinion, additional 10 days' time is sufficient for this purpose. We expect a response from the participating entities within 10 days specifying the portions (if any) of the report to which they may have an objection.

80. Insofar as the recommendations made by the Committee are concerned, we find that a proposal was mooted, that proposal was discussed and then an appropriate recommendation made. There are two categories of such recommendations. The first category is where there is a consensus between all the participants and the second category is where there is no consensus among the participants.

81. For the present, we request Mr Ajay Kumar to prepare ten sets of the proposals on which there is a consensus as well as the recommendations made on those proposals and separately ten sets of proposals on which there is no consensus in the recommendations made. The discussion held in respect of the proposals need not be included in those ten + ten sets. The sets will be given in a sealed cover (total twenty sealed covers) to the Court Master within three days and that be collected by the learned Advocates appearing for the participating entities as also Mr R. Balasubramanian, learned counsel for the Union of India. No one else will be entitled to these sets and we expect that the learned advocates will keep the contents of the proposals and recommendations completely confidential.

82. The learned counsel may discuss the proposals and recommendations with their respective clients and ascertain whether these proposals and the recommendations on which there is consensus and on which there is no consensus can be placed in the public domain.

83. We make it clear that since these are only 4 recommendations made, even if there is any objection by any of the participating entities, we will take a final decision whether the recommendations should be made public or not or whether they should be accepted or not. The participating entities will give their specific response within ten days.

84. For the present, we would like the participating entities, namely, Yahoo, Facebook, Google, Google India, Microsoft and Whatsapp to place on affidavit the number of complaints that they have received from India about objectionable contents concerning child pornography and rape and gang rape for the calendar year 2016 and 2017 from 1-1-2017 till 31-8-2017 and the action that has been taken (if any) on these complaints. This would be in addition to any suo motu action that the aforesaid entities may have taken even without any complaint having been received from anybody in India.

85. We make it clear that the details of the action taken need not be stated on affidavit. We are only concerned with the number of complaints received and the number of the complaints on which action has been taken.

86. The learned counsel for the petitioner submits that the Government of India through the Ministry of Home Affairs may file an affidavit indicating the number of prosecutions launched under Sections 19 and 21 of the Protection of Children from Sexual Offences Act, 2012 for the calendar year 2016 and 2017 from 1-1-2017 till 31-8-2017. The affidavit may also be filed within a period of ten days. List the matter on 18-9-2017 at 2.00 p.m.

(2018) 15 SCC 572

ORDER dated 18-9-2017

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

87. We have heard the learned Amicus Curiae and the learned counsel for the parties as well as Mr Ajay Kumar, Chairperson of the Committee appointed by this Court. Mr Ajay Kumar informs us that there are objections to some of the proposals and recommendations made by the Committee. He has prepared a chart of those proposals and recommendations to which there is an objection.

88. The learned counsel for the parties say that they would like to make submissions and substantiate the basis of those objections, but request that the hearing should be held in-camera. We have no objection in conducting the proceedings in-camera.

89. For the purpose of conducting the proceedings in-camera, the following steps need be taken:

(*i*) The Advocate-on-Record for the parties may obtain a copy of the report, both volumes, from their respective clients.

(*ii*) The Advocate-on-Record concerned will give a list of the Advocates and any person or persons representing any of the parties before us to the Court Master so that entry of any third party is ruled out. We make it clear that the representatives of the companies should be only from those who had participated in the discussions.

(*iii*) Mr Ajay Kumar has received a joint statement from the parties giving their objections to the proposals and recommendations being made

public. The learned counsel for the parties say that they endorse the joint statement. They will file an individual affidavit endorsing the joint statement and also indicating reasons for objections to the discussions being made public.

90. Presence of the learned counsel appearing for the States is dispensed with until further orders.

91. With regard to the second issue before us viz. the disclosure of the number of complaints that have been received, the learned counsel for the parties say that they require some more time to file an affidavit. The affidavit may be filed within two weeks.

92. The Union of India should file an affidavit indicating the number of prosecutions launched within two days.

93. List the matter on 23-10-2017 at 2.00 p.m. The hearing will continue the next day if necessary.

(2018) 15 SCC 573
ORDER dated 23-10-2017

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

94. On 18-2-2015, this Court had received a letter from NGO Prajwala to the effect that videos of sexual violence were being circulated in abundance.

95. After hearing the learned counsel for the parties, an order was passed on 22-3-2017[2] constituting a Committee to assist and advise this Court on the feasibility of ensuring that videos depicting rape, gang rape and child pornography are not available for circulation, apart from anything else, to protect the identity and reputation of the victims and also because circulation of such videos cannot be in public interest at all. We had expected the Committee to preferably arrive at a consensus on the possibility of ensuring that objectionable videos pertaining to child pornography, gang rape and rape are not made available on the internet. For some technical reasons, if that was not possible to explain and detail the reasons why it was not possible.

96. The Committee was constituted under the Chairmanship of Dr Ajay Kumar, the then Additional Secretary, Ministry of Electronics and Information Technology. The following persons participated in the deliberations of the Committee:

1. Shri Arvind Kumar, GC, Cyber Laws and e-Security, MeitY.
2. Dr Sanjay Bahl, DG, Cert-In;
3. Shri Rakesh Maheshwari, Scientist G, MeitY;
4. Shri Sunil Pant, Deputy Secretary, MHA;

2 Set out in paras 61 to 65, above.

5. Shri Chakit Swarup, Product Manager, Digital India, MHA;

6. Ms Aparna Bhat, Counsel for the Petitioner;

7. Ms N.S. Nappinai, Amicus Curiae;

8. Shri Vikram Langeh, Manager Trust & Safety, Facebook;

9. Dr Jim Hunt, Software Engineer, Facebook;

10. Shri Michael Yoon, Policy Manager, Safety & Content, Facebook;

11. Dr Anthony Surleraux, Child Safety, Google;

12. Dr Ksenia Duxfield Karyakina, Policy, Google;

13. Ms Gitanjli Duggal, Legal, Google India;

14. Shri Robin Fernandes, Grievance Officer, Yahoo;

15. Shri S. Chandrasekhar, Group Director, Microsoft;

16. Dr Radhakrishnan Srikanth, Group Program Manager, Microsoft;

17. Shri Balakrishnan Santhanam, Sr Program Manager, Microsoft;

18. Ms Keyla Maggessy, Law Enforcement Response Manager, WhatsApp;

19. Ms Gayle Argon, Legal WhatsApp.

97. The Committee commenced its proceedings on 5-4-2017 and met virtually on day-to-day basis. The Committee also took the advice of the experts who made presentation before the Committee. The experts are:

1. Ms Susie Hargreaves, CEO and Mr Fred Langford, Dy. CEO, Internet Watch Foundation (IWF), UK;

2. Professor Venkatesh Babu, IISc., Bengaluru;

3. Mr John Shehan, NCMEC, USA;

4. Shri Atul Kabra, Security Expert, FireEye, Bengaluru;

Certain inputs were also received from various other experts being:

1. Dr Hany Farid, Professor & Chair, Computer Science, Dartmouth College, USA.

2. Dr Mayank Vatsa, Mayank Vatsa, PhD, Adjunct Associate Professor, West Virginia, USA.

3. Dr C.V. Jawqaqhar, Associate Professor, IIIT, Delhi.

4. Prof. Dr Anderson Rocha, Associate Dean, Institute of Computing, University of Campinas, SP — Brazil.

98. Presentations and papers were also discussed by the Committee and the following presentations and submissions were made:

1. Presentation by Ms Aparna Bhat, Advocate for petitioner/ Committee.

2. Presentation by Ms N.S. Nappinai, Amicus Curiae/Committee Member.

3. Submission by Facebook representatives.

4. Presentation and submission by Google representatives.

5. Presentation and submission by Microsoft representatives.

6. Submission by Yahoo representative.

7. Combined industry submission of Google, Yahoo, Microsoft and Yahoo.

8. Presentation by Ministry of Home Affairs representative.

9. Written submission by WhatsApp.

10. Oral Presentation of NCMEC, USA and formal response to written queries.

11. Submission by Internet Watch Foundation (IWF), UK.

12. Presentation of Internet Watch Foundation (IWF), UK.

13. Presentation of Mr Atul Kabra.

The submissions of the learned Senior Counsel for WhatsApp Inc. were taken into consideration as well as those of the representative of WhatsApp who assisted the Committee. The following persons represented WhatsApp Inc.:

1. Mr Matt Jones, Software Engineer;

2. Ms Keyla Maggessy, Law Enforcement Response Management;

3. Mr Christian Dowell, Associate General Counsel.

Two members from WhatsApp Inc. viz. Ms Keyla Maggessy and Ms Gayle Argon were also co-opted in the Committee.

99. After a full discussion, a comprehensive report has been submitted to this Court by the Committee in two volumes. The second volume contains the presentations made.

100. We have gone through the contents of the first volume which deals with various issues that had arisen before the Committee. All the parties before the Committee agreed on certain recommendations based on proposals made during the deliberations. Part I of Chapter 7 of first volume of the Report contains the proposals in which the Committee was able to arrive at a consensus while Part II consists of the proposals in which the Committee was not able to arrive at a consensus.

101. We have been taken through the proposals as well as the recommendations made by the Committee on which there was a consensus.

102. We may note that Proposal No. 9 was actually dropped by the Committee. In other words, there are 11 proposals on which there is agreement between the members of the Committee and one proposal which pertained to WhatsApp Inc. being Proposal No. 18 which has been accepted while Proposal No. 19 pertaining to WhatsApp Inc. was dropped.

103. The proposals and the recommendations made on which there is consensus read as follows:

		Proposal	*Recommendations*
1.	(*a*)	The search engines expand the list of key words which may possibly be used by a user to search for CP content.	Government of India may work with the represented companies as well as civil society organisations to suggest expansion of the list of key words for showing CP warning ads/public service message on search.
	(*b*)	These key words should also be in Indian languages and vernacular search.	The same may be gradually expanded to other Indian languages where applicable.
	(*c*)	These key words should be expanded to cover RGR content.	For RGR, the Government of India may work with the represented companies as well as civil society organisations to suggest the list of key words for RGR warning ads/ public service message.
2.		Creating an administrative mechanism for reporting and maintenance of data in India.	
	(*a*)	Either within the CBI, or under the aegis of the MHA, a cell must be set up to deal with these crimes.	The Committee agrees that there is a need to create a Central Reporting Mechanism (India's hotline portal), as has been done in other countries, like in the U.S. with NCMEC. Further there is a need to strengthen law enforcement in this area. Any person/organisation should be able to report any CP and RGR content in India with ease with provision for anonymous reporting. This portal may go for INHOPE membership, as an Indian Hotline.
	(*b*)	A hash bank for RGR content be created (under the charge and control of Ministry of Home Affairs, GoI or through authorities or NGOs authorised by it).	The Committee also agreed that there is a need to develop a centralised agency to maintain and verify the hashes of all known CP and RGR imagery.
	(*c*)	GoI to formulate specific parameters for identifying RGR content to ensure expeditious identification and removal;	Government may look into these for appropriate action expeditiously.
	(*d*)	The hashes so generated must be under the custody of the centralised cell as stated hereinabove who will take to prosecute, as per the law.	
	(*e*)	A reporting mechanism must be created at a Central level, preferably with the CBI (in view of their role and special access) to also receive information of any CP/RGR content being circulated in the social media or any other platform over the internet.	
	(*f*)	The cell would regularly engage with represented Companies and the NCMEC for updation of technology, technical support etc.	

a		(*g*)	Technology similar to Project Arachind crawler technology be availed of, for identifying India — based CP and also to adapt the same for identifying RGR content online.	
b		(*h*)	Content hosting platforms (CHPs), Search Engines and GoI to work together in formulating process for proactively verifying, identifying and initiating take down of all CP/ RGR content.	
	3.		Project CCPWC being a general project to alleviate crimes against women and children, a special focus sub-project to be created within the same for eliminating CP\RGR to undertake the following.	
c		(*a*)	The Online Portal proposed to provide for anonymous reporting of identified CP/RGR.	Government may take action, as appropriate expeditiously.
		(*b*)	A separate hotline to be established for reporting (with the option for caller to remain anonymous) of identified CP/RGR content.	
d		(*c*)	GoI to identify and authorise specific authority/entity for receiving complaints of CP/RGR online and for initiating action thereon within specified timelines; such authority to have immunity and permission to verify CP/ RGR content and to initiate take downs: authority to also have specified processes for immediately intimating respective police stations for registration of FIR and for initiation of prosecutions.	
e				
f		(*d*)	A team to be set up for immediately verifying such tips and to issue directions to the service providers/intermediaries for immediate removal of such identified content.	
g		(*e*)	Government of India team/ authority to also immediately send communications to police stations concerned for registration of FIR and initiation of prosecutions. In view of the CBI's willingness to take this responsibility it is recommended that matter be handled by CBI and not by local police.	
h				

	(*f*)	Government of India to create tipper list of NGOs. Tips from such sources to be acted upon immediately by GoI authority for take down and initiation of prosecution without delay.	
4.		Creation of infrastructure/training/ awareness building:	
	(*a*)	Government of India to form regulations for reporting of identified CP/RGR imagery online.	Internet companies should provide technical support and assist in capacity building to the relevant agencies in India including law enforcement and NGOs through a series of trainings on online crime investigations, and trainings on using relevant internet tools.
	(*b*)	Government of India to ensure that search engines other than those already implementing URL blocks for identified CP/RGR content to initiate similar processes.	Internet companies should consider providing support to Indian NGOs to help bring awareness of these issues.
	(*c*)	Government of India or its designated authority/NGOs to be extended permission/immunity for human intervention to identify CP/ RGR content.	Government of India may also conduct regular training programme as well as relevant Government training infrastructure to have the latest technology on the subject-matter.
	(*d*)	Government of India to allocate funds for training, verification, continuous monitoring and review of personnel involved in such human intervention process for identifying CP/RGR content, in line with those adapted by NCMEC/IWF.	Government of India may also partner with civil society organisations, research institutes to conduct programme as mentioned in (*c*) above. Premier research institutes like IISc must be encouraged and supported to have dedicated research programme to undertake these studies.
	(*e*)	GoI/CHPs/search engines to involve in creation of awareness amongst users and sensitisation programs and capacity building initiatives for judiciary, prosecutors and law enforcement authorities, to mitigate the menace of CP/RGR dissemination.	
	(*f*)	GoI to set up processes for expeditious initiation of prosecution against users for identified CP/RGR content reported by CHPs.	
5.		The solution lies in proactively identifying rogue sites by an independent agency which can identify sites that contains CP and	The members of the Committee were of the opinion that this could be a process that could be considered for suitable implementation in India.

			RGR content and blocking these sites. To prevent the circulation of subject imagery, Government can block any additional sites/ applications if they do not remove such contents of their own. MHA/ designated LEA can be empowered to directly order Indian ISPs through DoT.	
	6.		The Government, through an appropriate agency setup a VPN to receive the NCMEC reports for uploading of CP from India. As conveyed by NCMEC, there were more than one hundred thousand reports belonging to India. Law enforcement agencies should initiate legal action against uploaders.	The Committee agreed that this should be looked into expeditiously.
	7.		*Removal of known CP/RGR imagery*: When imagery is detected as CP/RGR, in addition to preventing subsequent uploads, content hosting platforms (CHP) voluntarily identify, remove and prevent distribution of previously existing content on their platforms.	The Committee agreed to the said proposal.
	8.		There is need for greater thrust and emphasis on research & development of Artificial Intelligence (AI)/Deep Learning (DL)/Machine Learning (ML) based techniques for identifying CP/RGR content at the stage of uploading to enable real time filtering. Some specific suggestion in this regard may include as follows.	The Committee recognised the technologies developed by represented companies including PhotoDNA, Video hashing and other techniques for Imagery. However Committee also recognises the need for much greater collaborative work in the subject area amongst all stakeholders.
		(*a*)	Traditional DL/ML techniques, including feature engineering based techniques and other Image processing techniques to be developed for identifying CP/RGR content at the stage of uploading.	The Committee also feels that video hashing technique should also mature as has been done for hashing techniques for images. Represented companies should further voluntarily collaborate with NCMEC to establish a shared database of CP video hashes similar to the image hashes database that is already used by the industry.
		(*b*)	CHPs to review existing architecture to screen/verify uploads for CP/ RGR content using such AI/DL/ML tools after suitable technologies are developed.	
		(*c*)	AI/DL/ML tools to be tested real time (i.e. upon each upload).	The committee suggested that suitable research be initiated for further development of technologies for identifying CP/RGR imagery.
		(*d*)	Research into above alternatives to be initiated in a time-bound manner.	

	(*e*)	CHPs to consider using NCMEC for creating deep learning/machine learning tools, subject to applicable laws, for CP (to avail of the huge data sets repository of NCMEC).	
	(*f*)	Government of India, along with CHPs to engage services of suitable experts for developing deep learning/machine learning tools for identifying RGR content.	
9.		*User authentication*: Create a mechanism where users who seek to upload an image/video, falling within the subject content, using the pre-identified key words, are put to a more rigorous verification process which would have them believe that they would be traced.	The Committee decided to drop this proposal by consensus.
10.		Content removal processes/URL de-indexing process for identified RGR imagery should be as expeditious as removal of CP imagery.	The represented companies stated that they are continuously working on improving processes for review of content including RGR that is reported to them. The Committee noted the same.
11.		Content hosting platforms, social media platforms and search engines will provide links for reporting CP/RGR imagery, as a specific category and the same to be more prominently displayed on their pages.	The represented companies stated that they are continuously working on improving processes for reporting content including CP and RGR that violates their policies or applicable laws. The Committee noted the same.
12.	(*a*)	Create a mechanism to ensure that when CP imagery is identified, the CHPs shall preserve and retain such information of the uploader including the identified content to assist law enforcement.	The represented companies are already taking action in this regard. The Committee agrees to Part (*a*) of proposal.
18.		WhatsApp should make further improvement in their reporting process which would enable easier reporting of contents in the App while maintaining the integrity of the contents and metadata available on phone at the time of reporting.	There was consensus in the Committee. The Committee recommends that these efforts be taken up at the earliest.
19.		Compute the PhotoDNA has, VideoHash at WhatsApp Client on Mobile Handset level, and transmit them to central WhatsApp server for matching with CP/RGR Hashes database.	The Committee agreed not to pursue this proposal.

104. We expect the parties including the Government of India to abide by the recommendations on which there is consensus and to try and implement

them at the earliest. We make it clear that any information that is based on or is pursuant to the proposals and recommendations to the Government of India will be kept confidential so as not to reveal the technology used by the participating service providers.

105. The Government of India will prepare a status report on implementation of the recommendations and place it before us in a sealed cover before the next date of hearing. On the next date of hearing, we will deal with the proposals on which there is no consensus.

106. List the matter on 11-12-2017 at 2.00 p.m. It is made clear that on the next date of hearing also the proceedings will be held in-camera.

(2018) 15 SCC 581
ORDER dated 11-12-2017

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

107. The learned counsel for the Union of India has handed over a status report. Unfortunately, on going through the status report, it is found to be more in the nature of comments rather than a status report. We expect the Union of India to file a proper detailed status report rather than comments on the orders passed by this Court.

108. The learned Amicus and the learned counsel for the petitioner have concluded their submissions with regard to Proposal 12(*b*) and Proposal 13. The matter may now be listed on 8-1-2018 at 2.00 p.m. for submissions on behalf of the learned counsel for the intermediaries with regard to Proposal 12(*b*) and Proposal 13.

109. It is stated by Col. R. Bala, learned counsel appearing on behalf of the Union of India that a portal has been prepared for making complaints by citizens with regard to issues pertaining to child sexual abuse, child pornography and rape/gang rape videos. The learned counsel for the Union of India says that the portal will be ready within a month. He further says that standard operating procedures are being prepared for use of the portal.

110. The learned counsel for the petitioner says that the portal should be given adequate publicity so that people can make complaints. She says that there should also be a provision for making a complaint anonymously. Col. R. Bala, learned counsel says that he will advise the Union of India accordingly.

111. The matter has been pending for quite some time and we find from the affidavit filed by CBI on 8-10-2015 that steps are being taken to enable complaints being filed through a portal. It is high time that the Union of India gets the portal ready and available to the public at large. Therefore, we direct that the Union of India to have the portal ready on or before 10-1-2018. We would like the report to be given on the next date of hearing i.e. 8-1-2018 with regard to the progress made. It is also made clear that on the next date of hearing also the proceedings will be held in-camera.

(2018) 15 SCC 582

ORDER dated 8-1-2018

(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)

Suo Motu WP (Crl.) No. 3 of 2015

112. We have heard the learned counsel for the parties and the learned Amicus Curiae.

113. The learned Additional Solicitor General has placed on record a status report in the matter of videos of sexual violence and recommendations. It is stated in the status report, inter alia, that the Ministry of Home Affairs has identified the keywords for child pornography/rape and gang rape content search and a list of keywords in English language has been compiled and circulated to content providers for further action. Efforts are being made to update the list on regular basis. It is orally submitted before us that the keywords in other languages will also be taken up for consideration in due course of time.

114. It is further stated that online cyber crime reporting portal has been developed with access name as www.cyberpolice.gov.in and that this portal is undergoing security audit and has been deployed in staging environment for testing and trial. It is expected that it will be operational very soon. It is further stated that certain features will be made operational by 10-1-2018 and offered to public such as anonymous reporting of child pornography/rape/gang rape content and online registration of cyber complaints which will be forwarded to the State/UT police authorities concerned for appropriate action.

115. It is also stated that certain other features are likely to be made operational by 10-2-2018 with regard to providing status update of complaints to registered complainants, portal access to other stakeholders willing to register for providing inputs on child pornography/rape/gang rape content and maintaining hash tag of obscene content.

116. For the time being, we adjourn the matter to 15-2-2018 at 2.00 p.m. so that we are made aware of the progress made by the Union of India in this regard. Further orders will be passed after the hearing on 15-2-2018.

117. It is stated by the learned counsel for the petitioner that her impression is that Facebook is developing or has developed new "proactive detection" technology for real time screening through artificial intelligence. In this regard, the learned counsel appearing for Facebook may file an affidavit indicating whether any such technology has been developed and if it has not been developed the progress made for developing such technology, if any.

118. The affidavit be filed within three weeks. List the matter on 15-2-2018 at 2.00 p.m. It is made clear that on the next date of hearing also the proceedings will be held in camera.

(2018) 15 SCC 583 (1)
ORDER dated 15-2-2018
(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)
Suo Motu WP (Crl.) No. 3 of 2015

119. It is submitted by the learned ASG that with reference to order dated 8-1-2018[3], some more time is required for completing the exercise and putting a portal in place so that it is fully operational and responsive. The learned ASG says that it will take about four months' time for this exercise.

120. According to the learned counsel for the petitioner, it would be more appropriate if some sort of a road map is placed on record by the Ministry of Home Affairs so that there is some clarity on how the exercise is progressing. The learned ASG says that the road map can be prepared and filed within two weeks.

121. List the matter on 12-3-2018 at 2.00 p.m. However, it is made clear that the road map should be circulated immediately after two weeks.

Report of the Special Committee

122. We have heard the learned counsel for the parties. It appears to us that it would be appropriate if all the parties can sit down together with the learned Amicus Curiae and the proposals before the Committee where there was no consensus can be classified into administrative proposals and technology related proposals. Once this identification is complete, which we expect will be agreed upon by all the learned counsel, appropriate directions can be issued by this Court.

123. Needful be done within two weeks. List the matter on 12-3-2018 at 2.00 p.m. as first item.

(2018) 15 SCC 583 (2)
ORDER dated 12-3-2018
(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)
Suo Motu WP (Crl.) No. 3 of 2015

124. A road map has been given by the learned Additional Solicitor General in the form of a status report. The learned Amicus Curiae has also given her submissions and a list of proposals about which there is some partial disagreement. The learned Additional Solicitor General says that the Ministry of Home Affairs would look into this and implement the road map and administrative issues at the earliest.

125. List the matter on 16-4-2018 at 2.00 p.m. as first item. It is made clear that on the next date of hearing also the proceedings will be held in-camera.

(2018) 15 SCC 583 (3)
ORDER dated 16-4-2018
(BEFORE MADAN B. LOKUR AND UDAY U. LALIT, JJ.)
Suo Motu WP (Crl.) No. 3 of 2015

126. We have heard the learned Amicus, the learned ASG and learned counsel for the parties.

3 Set out in paras 112 to 118, above.

127. A very brief status report has been presented in the Court today. On going through the brief status report, we find that the Ministry of Home Affairs has committed itself to open the Beta version of the portal for online cyber crime reporting. The public launch of the Beta version is expected in the last week of April 2018.

128. It is also stated that connectivity of the portal has been tested with Maharashtra, Kerala, U.P. and Chandigarh. The process is underway to establish connectivity with all other States/UTs and efforts have been made to integrate as many States as possible before the launch date.

129. Our attention has also been drawn to the recommendation made by the Committee against Proposal 2 which is to the effect that there is a need for a Central reporting mechanism as has been done in other countries particularly in the United States. Orally, we have been told that some progress has been made in this regard but this is a very scattered sort of submission made before us.

130. We have also been informed by the learned counsel for the parties that there are several other Ministries that are interested in similar issues such as the Ministry of Women and Child Development. The learned ASG informs us that the Ministry of Electronics, Information and Technology is also interested in taking corrective steps insofar as cyber crimes are concerned particularly those relating to rape/gang rape/child pornography.

131. It would, of course, be in the interest of all concerned if the Central reporting mechanism is set up. Orally, we have been informed that some sort of systems are in place.

132. We would like to have a comprehensive and detailed status report from the Ministry of Home Affairs informing us about the progress made keeping in view the fact that there is a road map already indicated in the affidavit dated 1-12-2015 and other subsequent affidavits. The status report will deal with all these issues in a comprehensive manner.

133. We would also like to know from the parties before us before the next date of hearing about the status of progress made pursuant to the recommendations accepted by these entities as mentioned in the Report of the Committee.

134. List the matter on 11-5-2018 at 2.00 p.m. as a first item. It is made clear that on the next date of hearing also the proceedings will be held in-camera.

Court Masters