TREADING THE TIGHTROPE: BALANCING CYBER SECURITY WITH FREEDOM OF SPEECH AND EXPRESSION

by

AKSHAY | Student of 4th Year, B.A., LL.B. (Hons.) | Amity Law School | GGSIPU Delhi
akshaypathak.123@gmail.com | B/71, Sagamlok Apartment, Buddha Colony, Patna

ABSTRACT

There’s a wonderful line in Stephen Chomsky’s novel ‘The Perks of being a wallflower’ in which a character mumbles that the biggest irony of the internet is that it has brought the world closer, but not the people together. This quote clearly crowns the apprehensions of cyberspace many of us have today. Cyberspace is a vast plethora of opportunities, one which like anything else in the world comes with a lot of trepidations. Today in India, the debate rages whether we need to regulate and censor what our citizens’ post on their walls and what our kids see on the tube. However, censorship doesn’t go hand in hand with the free, democratic nature of the Indian state. Essentially it contravenes the fundamental rights guaranteed to the citizens by the Constitution of India. But what adds to the fire is that now, these dictums of the Constitution do not stand against the Government’s determined stand to monitor content especially as the riders like national security do not even come in the picture.

KEYWORDS: This research paper shall examine the various cyber crimes cyber-censorship and its conflict with the Constitution of India.

INTRODUCTION

Cybercrime are the crimes related to information technology, electronic commerce etc. The cyber frauds, hacking, obscene material, viruses, harassment, violation of privacy, intellectual property violations, cracking etc., are increasing in all the countries rapidly and it is expected to provide a new dimension to the existing cyber laws and other provisions. On one hand the advent of internet has proved to be a boon to the professionals, on the other hand, its unregulated nature has created a fertile ground for criminal enterprise. Web crime statistics: Total complaints filed in 1993 for cyber crimes was 640(1.7 per day), it went up to 971(2.6 per day) in 1994 and to 1494 in 1995, to 4322 in 1996, to 12775 in 1997, to 47000 in 1998 and to almost 1,00,000 in 1999. In the present scenario, the situation is such that it’s nearly impossible to find out exact data for cyber crimes. “Norton Cyber Crime Report 2011” reveals that the total number of cyber crime victims touches 431 million. It is in light of the above statistics that the state has taken an initiative to censure or as it says ‘pre-screen and monitor content for the greater good of the society.’ The amended IT act, 2008 allows or rather gifts the government with draconian powers that allows it authority to unilaterally monitor, regulate content on web
servers and internet in general. This censuring and e-surveillance of web content is a heatedly debatable one as not only does this contravene Article 19 of the constitution but arising from the world’s largest democracy it’s simply shameful. Not only does this dilute the principle of freedom of speech and expression but it also denies the citizens of the State with the many avenues of information in cyberspace.

**CYBER CRIMES: CLASSIFICATION**

Donn Parker identified four forms of computer abuse namely: 1) computer might serve as the victim of the crime 2) computer might constitute the environment within which a crime is committed 3) computer might provide the means by which a crime is committed 4) computer might symbolically be used to intimidate, deceive or defraud victims. It is of utmost importance to discuss the various cyber crimes.

Talking specifically about cyber crimes, they can be classified as:

- Unauthorised access
- Cyber fraud
- Hacking
- Cyber theft
- Cyber terrorism
- Cyber pornography
- Alteration and destruction of digital information

**UNAUTHORISED ACCESS**

Knowingly or intentionally use or access without the permission or consent of the owner or possessor whole or any part of a computer, computer network, system is unauthorised access. It can be compared to criminal trespass defined in section 441 of the Indian Penal Code. Section 65 of the Information Technology Act 2000 in India prohibits tampering with computer source documents and prescribes punishment. It reads as-“whoever knowingly or intentionally conceals, 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.” Even the Computer Fraud and Abuse Act was revised in 1994 and amended in 1996 to curb cyber crime in the U.S.A. The Act prohibits unauthorised access to information and protects confidential information. After the R. v. Gold, case of computer hacking, the computer misuse act was passed. Section 1 of the Act made obtaining unauthorised access to computer programme or data the basic offence.
CYBER FRAUD

Cyber fraud is a crime whose growth has been as rapid and diverse as the growth of the internet itself. The consumer organisation, Internet Fraud Watch declared that the number of consumer complaints regarding the cyber fraud rose dramatically from 1,152 in 1997 to more than 7500 in 1998. This itself indicates the seriousness of the issue of cyber fraud and the need to curb it. It is very easy for the fraudsters to make their messages look real and credible, but it is almost impossible for the people accessing internet to tell the difference between fact and fiction which adds on to this problem. Section 25 of the Indian penal code defines the word fraudulently as “a person is said to do a thing fraudulently if he does that thing with intent to defraud but not otherwise.” The Information and technology draft bill 1998, in section 63(1)(g) includes such fraudulent acts and makes it a crime.

HACKING

Clause 66 of the IT Act defines hacking as:

“whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.”

The Computer Misuse Act, USA, the Computer Fraud and Abuse Act 1984 prohibit hacking. Section 65 and 66 of the Information Technologies Act 2000 also prohibits hacking. The term “Hacking” is a very broad term and there are various types of hackers specialised in specific areas and they use their skills to their advantage.

Kinds of hackers:

- Code hackers- They can make a computer do almost anything.
- Crackers- They circumvents operating systems and their security.
- Cyberpunks- Masters of cryptography.
- Phreakers- They combines their in-depth knowledge of the internet and mass telecommunications systems.
- Ethical Hackers: Ankit Fadia and Dr. Neruker in India were identified by NASSCOM and Law Enforcement Agencies as ethical hackers who work for cyber security and co-operate with the government to prevent and control cyber crimes.

Some hackers just enjoy cracking systems without any malafide intention. Such act can perhaps, most appropriately be considered in the light of laws relating to criminal trespass. Section 441 of the IPC mentions trespass.
Whether websites are property??

The common law action of trespass to real property served to establish and preserve the very notion of “property” in land. Many of the words used to describe a website have a basis in real property; the word “site” itself is one, as are other expressions such as “home”, pages, “visiting” to a site etc. So therefore, the usage of such word itself suggests that the trespass action might appropriately be applied to websites as well. Another question that is of vital importance is that when a hacker has no intention to commit any further crimes, whether such hacking is enough to constitute intimidation or annoyance. It has been clearly laid down in Smt. Mathri v. State of Punjab that for establishing the offence of criminal trespass it is not enough to merely show that the person entering upon the property of the other had the knowledge that his act would cause annoyance. The rule that the person must be presumed to intend the natural consequences of his act is not a binding rule, if any other intention can be shown.

**CYBER THEFT**

There have been instances where people have been denied financing because of insufficient credit limit because there have been credit cards opened on his/her name for which they never applied. This is a case of identity theft. In such cases the victims don’t even realise that their identity has been stolen by someone else. The Identity Theft and Assumptions Deterrence Act or the Identity Theft Act was enacted on 30th October, 1998 to prevent and control Identity theft or cyber theft. In 1998, in support of the Identity Theft Act, The General Accounting Office (GAO) published a report called “Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited.” The report stated that the Social Security Number (SSN) misused increased from 305 in 1996 to 1153 in 1997.

**CYBER TERRORISM**

“Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.” There have been reports of the terrorist groups making fresh recruitments through internet. Internet is something that would continue to dominate in terror circles and, these groups will continue to use the internet as their prime medium to both recruit and more importantly communicate with each other. Ronald Noble, former head of the United States secret service who is now the secretary general of the Interpol says in an interview in the Independent that the internet is giving terrorists new ways to plot mass murders. Despite such awareness, laws and tight vigilance they always manage to put across their point to their fellow operatives using the internet. Amendments under the Information Technology Act, 2000 has defined the term “Cyber-terrorism” Under Sec. 66F. This is the first ever attempt in India to define the term. Whoever commits or conspires to commit cyber terrorism is punishable with imprisonment which may extend to imprisonment for life. i.e. imprisonment not exceeding fourteen years (Sec. 55, IPC) This Section has defined
conventional Cyber attacks like, unauthorised access, denial of service attack, etc, but as discussed above, motive and intention of the perpetrator differentiates the attack from an ordinary to an act of terrorism.

**CYBER PORNOGRAPHY AND CHILD PORNOGRAPHY**

There is no settled definition of pornography or obscenity. Pornography or obscenity is very sensitive issue all over the world yet there is no settled definition of the word under any law. Pornography uses parameters such as obscenity and indecency which are controversial. The Supreme Court in Abbas v. Union of India recognised that standard of morality is not uniform or flexible standard but varies according to different communities or ages as well as a number of historical, ethnic and social conditions. However, Section 67 of the IT Act, 2000 penalizes cyber pornography. Section 67 reads as under:- “Whoever publishes or transmits or causes to be published or transmitted 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 three years and with fine which may extend to five lakh rupees and in the event of 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.”

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. Dr. R.L Prakash case on cybercrime is very significant where the court convicted the accused under Sec 67 of the IT Act, 2000. The accused was arrested by the Chennai police for making cyber pornographic images of his clients forcefully.

**ALTERATION AND DESTRUCTION OF DIGITAL INFORMATION**

Flowing programmes through computer network by human agent such as virus, Trojan horse, worms, logic bombs, to cause damage, alter, delete , destroy computer, computer system, computer database are also cyber crimes. A computer virus is a programme designed to replicate and spread generally with the victim being obvious to its existence. Computer viruses spread by attaching themselves with other programmes or to the boot sector of a disk. When an infected file is activated or executed, or when the computer is started from the infected disk, the virus itself is also executed. A Trojan is a malicious security breaking programme that is disguised as something being, such as a directory lister, game or even a programme to find and destroy viruses. And a worm is a programme that propagates itself over a network, reproducing itself as it goes. In the case of R. v. Thompson the court held that logic bomb is a kind of imputation of a programme or a code inserted into an application or operating system that causes it to perform some destructive or security-compromising activity wherever specific conditions are met.
CENSORING CYBERSPACE

“Censorship signifies a society’s complete lack of confidence in itself.”

One of the early nicknames of Internet, some months after it came to the public was the ‘information superhighway.’ For people who were accustomed to getting to know about stuff through the common media of radio, newspapers and even, television, the internet opened up new avenues of a world of information. The internet became a paradise for those seeking help, opinion and even ideas over any issue. The world as it was, came closer and stood connected as the invisible lines of the World Wide Web bound the globe in a close knot. What happened in the USA could be learnt in China in a matter of minutes, what a guy spoke in India could be heard miles away down under. This is what the phenomenon of internet gave us, a sense of being closer to the rest of the world than ever and knowing that no place on earth is too far.

However like any of man’s greatest inventions and discoveries. The latest and probably the most prominent being is the call for censoring the avenues of cyberspace. Censorship may be defined as “the control and suppression of information and ideas circulated in a society.” Derived from the Latin word ‘censure’, it originally meant a magistrate who undertook census in the ancient Roman Empire. Needless to say, it was quite a different strand of meaning than it is now. The supporters of Cyber censorship has often been justify it by considering it as a protection against hate speech, pornography, obscenity etc. Of late, India too has been a centre of the censorship pogrom. There are voices, many of them who wish to suppress the degree of information that flows freely on the social media and other elements of cyberspace. However, before looking at India it is important that censorship as an issue be taken. Its history and evolution in other parts of the world.

CENSORSHIP IN SOCIAL NETWORKING SITES

Of late, a raging furore was caused by the Former HRD Minister Kapil Sibal’s intention or rather prospect of regulating and monitoring content on the internet, especially those social networking sites owned by internet companies like Google, Facebook and Twitter. Unlike ISP’s, internet companies are not quite conforming resulting a steady rise in anti-state revivalism in India.

The government states that it is ”strengthening the Internet as a vehicle for openness, democracy, inclusiveness and unhindered access to information and knowledge,” by making it a cleaner forum for the people to access. They also justify their move to try censoring the internet by saying that of late, the social media has been used to ferment trouble between groups. True, however one can’t deny that the internet being a open forum has it’s variance of pros and cons. Everyone is entitles to his own opinion and even if one’s opinion hinders others, social networking sites like Facebook do have regulations in place to keep in check and monitor content. In hindsight though, it seems that the move to censor such sites are a way to get back at dissidents as most of the websites that were asked to be removed were critical of the ruling government. So, the question arises
whether the internet and cyberspace is becoming an instrument of state control. This was further enhanced by India making a proposal for Internet Regulation at the Global Internet Governance, ICT of the UN. For a nation that calls itself a democracy, this is a shame.

INDIA’S TRYST WITH CENSORSHIP

"D.E.M O’Cracy beloved husband of T.Ruth, father of L.I.Bertie, brother of Faith, Hope and Justice expired on 26 June”.

This infamous obituary in the Bombay edition of the Times of India, way back in 1975 possibly was the most iconic statement against the imposition of Emergency by Smt. Indira Gandhi. It was a time when ‘democratic’ India lost its meaning and lost out on what it she stood for. It was a time when wagging tongues were rolled back in and sycophants rewarded with sweets. Simply speaking, there was complete curtailment of freedom of speech and expression, especially those that didn’t meet the favor of the government.

India has a long history of censorship, even if it’s not as storied as its Asian compatriots. Bollywood movies like ‘Aandhi’ and ‘Kissa Kursi Ka’ were banned for overtly political tones. So, were plays like ‘I am Nathuram Godse Speaking’ and books like Rushdie’s ‘Satanic Verses.’

However, cyberspace censorship is a recent trend in India. Or rather, a more debated upon and controversial trend. Even today, hardly 2% of India’s population has internet access. However, it must be noted that these 2% constitute the urban middle and higher class who have the loudest voices in the political and social spectrum.

The earliest instance of Cyber censorship in India was the banning of ‘Dawn’, a Pakistan-based news agency’s website in the aftermath of the 1999 Kargil War. Other instances included the blocking of specific yahoo groups and the government’s agreement with Orkut to block defamatory content critical of religious, political leaders.

However, the debate on Cyber censorship is a more recent debate especially in the aftermath of the heinous 26/11 attacks in Mumbai. We have a state, that now has unlimited monitoring and regulatory possibilities even if it wears the mask of ‘freedom’ hidden behind the provisions of the Constitution. We have a public, who opposes the draconian hand of the government but falls short of being vehemently critical of the same. And we have a law, namely the amended IT Act which is more autocratic, abusive and restrictive which in essence is shameful of the world’s largest democracy.

It must be noted that such measures of the State come in the aftermath of increasing cyber-attacks on Indian internet servers and communication services from both across the borders and from within. India is one of the largest growing virtual populations in the world which makes it increasingly prone and vulnerable to forces that it may not be able to control and monitor. In such a case, we need a state that is more focused on catching and bringing to justice cyber-criminals who threaten national security and not target its own citizens who may have to look over their own shoulder every time they post their blog or
post on their wall to see if big brother is watching. Proactive self-defence in cyberspace is needed not only against alien enemies but also against our own Orwellian government.

Also, we have a state that proposes to initiate a Central Monitoring System, something on the lines of the Supreme Council of Virtual Space in Iran. This proposal, without any parliamentary approval not only contravenes the democratic and reconciliatory nature of the Indian constitution but also includes draconian measures in it such as the Internet kill switch, which not only is an unconstitutional recourse by the State but may not always be a solution to cyber threats. Also, of late there has been increasing government interference in the activities and functions of domains and websites, especially those concerning social networking. Recently, the government had asked Google, Yahoo, Facebook and Twitter to pre-screen contents before they were posted to the public. Not only is this proposition ridiculously preposterous but is also another step for the government up the ladder of autocracy. In other words, if recent events are anything to go by it won’t be too late that India moves from a welfare state to a police state.

Self-defence in cyberspace is a concept whose time has come at both national and international level. At the centre, we need to safeguard ourselves from not only despicable cyber criminals but also against our very own overenthusiastic state that indulges in a labyrinth of e-surveillance and content regulation measures. At the international level, we need to safeguard ourselves against forces across our borders, especially as there are increasing incursions into India’s cyber security sphere. This is in the light of increasing Chinese influence in the subcontinent and its clandestine attempts to circumvent Indian cyber security over the years.

As the world’s largest democracy, we must make sure that it stands by what our founding fathers envisioned it to be. We don’t have a perfect state or a perfect people, but they are all we’ve got and it is up to us that we stand by the dictum of freedom that our nation upheld on the eve of our independence.

CONFLICT BETWEEN CYBER CENSORSHIP AND FREEDOM OF SPEECH AND EXPRESSION

Since it was drafted in the wake of a torrid independence, the Constitution of India has had a long, storied history of being an inspiration for other democratic states of the world, most notable South Africa. However, the primary ideal by which our constitution supposedly stands by has come under a lot of fire of late.

The Article 19(1) of our Constitution guarantees that every citizen, regardless of any distinction and territory shall enjoy the right of freedom of speech and expression. The question thus arose, quite early in India’s democratic history that whether other important state institutions like the press enjoyed this right. They do, as held by the Supreme Court in Ramesh Thapar v. State of Madras as they form a part of the essential democratic associations.
However, recent events have brought into question the Indian state’s commitment to ensure its citizens the same right it celebrates. For example, while the whole nation was swept by a strong anti-corruption wave, India had quietly introduced a proposal of internet regulation at the ICT, the UN body for Internet governance. India proposed such a plan in order to ‘restore openness and unity in democracies.’ However, what it thinks to be a right step may turn into a bad fall into an abyss. The media and the internet are a vast forum with unlimited possibilities and any step to try censor it is futile.

More importantly, for a democracy India seems quite ready to take away from its citizens their primary right. The State says that proposes such step in order to avoid any defamatory content and protect our children. Here, the government is faulty at two instances. First, the definition of defamatory itself isn’t justified as what is seditious to one may not be the same for another. Also, why should there be any step to censor cyberspace when simple parental controls would suffice to protect what our children see on the Internet. Censorship is a step that may look good on paper in terms of greater good, but essentially it is a proposal for the deprivation of liberty. Not only will the ‘big brother’ government be stifling different voices and opinions, it is also reducing to incentive of wisdom by suggesting the decline of individualism in a democratic society. As quoted by Meiczyszaw Maneli, “Wherever there is a loophole in the existing laws protecting liberties, the opponents of these freedoms try to squeeze in. Whenever legislators create the slightest opening to allow some kind of censorship, the censors will be born and will march again.” And as the furore over this goes on, one must also consider whether censorship is an instrument for those in power to retain their chair.

As a nation with a brilliant constitution at hand, we pride ourselves at being able to talk, express and move about freely with few limitations. However, when these key rights are taken away from us, especially those inconsistent with our constitutional guarantees, in the name of ‘greater good’ not only are we bound, but so is our progress is the pursuit of life, liberty and happiness.

CONCLUSION

As already discussed in this paper, the Internet in all its glory is the napoleon of modern-day communication. Not just is the world closer, but it is actually just seconds away and has demystified the hassles of distance in the world. It has also been established that like anything good, too much of it can be bad. And as we know it, the vast virtual space has led to increasing exposure of people to content on the internet and has led to rising degree of cybercrimes. However, what must be understood accurately is the fact that the internet is not to blame for the same. It’s primarily a medium of communication, a forum where the unheard can make their voices heard and where diversity has a name. In U.S District judge Stewart Dalzell’s words, ‘the internet provides a common platform for all to speak and brings about relative parity among the speakers.’ When we talk about cybercrimes and censorship and the debate that ferments it, we must ask ourselves whether Internet censorship is appropriate. We must understand that the Internet is not a different place, but
a reflection of how the people and society stand in the real world. Plus, wrongful content isn’t something one finds only in the internet, but forms an incorrigible part of our very society. If we say that the internet is dirty, so are the people who contribute to it. Here, censoring the internet may look feasible on the face of it to prevent any hate speech, defamation, fraud or in case of India, any communal incitement. However, it must be understood that to censor the internet would be to stifle the citizens of the State themselves. As Indian citizens, we are blessed with the freedom of speech and expression, that which inalienably extends to the virtual space. However, if the State moves to censure its own people, all these constitutional guarantees stand void and as a democracy, that is something to be ashamed of. As a growing global power, India must strike a balance between the issues at hand because any step taken by the State shall become obsolete in the near-future with rapid contextual and elemental changes in technology and society. And if we go ahead with censoring cyberspace, we’ll only go back as square one.

REFERENCES


