Page 106 - 122 DOI: https://doij.org/10.10000/IJLMH.112811

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 2

2022

Information Technology vis-a-vis Human Rights: An Analytical and Legal Approach

Aarzoo Agarwal[1]

Abstract

The explosion of information and communication technology has been the most influential element in the globalisation process. So much have computers invaded every aspect of life, and so quick has been the impact that the institutions of law and justice have been caught unawares. IT has acted as a double-edged sword as, on the one hand, it has benefitted immensely, but at the same time, one of the rising problems is its relation in violation of human rights.

The IT legislation arena is a comparatively new field that requires a detailed study into its formulation, strategic development and continuous evaluation in the era of advancement of artificial intelligence and technological dominance. The need of the hour is to analyse the rapid advancement in information technology in the context of the dilapidated and gradual growth of the existing framework of IT legislation and its juxtaposition with Human Rights at the international as well as the domestic level and arrive at a balancing position with regard to the abovementioned inter-related aspects. This calls for the drafting of effective policies, actions and legislation to combat issues arising from the unbridled advancement in technology which in many ways leads to the blatant breach of human rights.

I. Introduction

Cyberspace can be thought of as a global electronic village that cannot be spatially located and is composed of intangible objects such as social networks, personal information and reputation, email accounts, websites etc., where there exist no geographical barriers and facilitates instantaneous communications.[2] Similar to the existence of a bad aspect to anything and everything good, cyberspace and the advantage and level of convenience that it has provided to the world around, has also led to massive growth in cybercrimes, which encompasses any crime involving a computer network or system. With the help of the information obtained through a computer, illegal activities such as online transactions, which are unethical, credit

[1] Author is an Advocate at Siliguri District Court, India.

[2] The term 'global electronic village' was coined by Marshall McLuhan in his books 'The Gutenberg Galaxy: The Making of Typographic Man'(1962) and 'Understanding Media'(1964).

card frauds, violation of intellectual property rights, destruction of information, online theft and even physical sabotage or abuse may result.

Cybercrime cannot be defined in absolute terms because of its extremely wide horizons. To cite an interesting instance, even a petty offence like pickpocketing and stealing can be brought within the wider purview of cybercrime if a computer or any information stored online serves as an aid in any way to the commission of such an offence. In the Indian context, neither the Information Technology Act, 2000 nor the National Cyber Security Policy, 2013 or any other regulation defines cybercrime in a concrete form. However, such offences or crimes have been dealt with the listing of various individual acts and the related punishments under the Indian Penal Code 1860 and quite a few other legislations.

Misuse of IT has led to various risks to individuals, organisations as well as governments.[3]

- Individual risks such us to online defamation, cyberstalking, identity theft, net extortion and cyberbullying.
- Financial risks such as credit card fraud, phishing, etc.
- IPR violations like software piracy, copyright violations, cybersquatting and trademark infringement.
- The risk to computers and safeguarded data through viruses and email spamming.
- Increase in online illegal activities and crime through the sale of illegal items like drugs, pornography and gambling.
- Risk to States and governments through cyber warfare, cyber spying, cyber terrorism, violation of confidential information privacy, and also hacking of online government websites.
- Check to individuals by online defamation, cyberstalking, fraud, net extortion, cyberbullying and identity theft.[4]

II. THE INFORMATION AGE AND IT LAWS

In this era of rapid advancement in technology, information is being cited as the new gold. Data, when processed into information, has immense potential to alter the way things run around us. Since the creation of the cyber world, much of how the world runs depends on the use of information technology. Business, education, and even health care have been redesigned to adapt to rapidly developing facets of work and life. Post the onset of the CoViD pandemic,

[3] ANIRUDH RASTOGI, "CYBER LAW- LAW OF INFORMATION TECHNOLOGY AND INTERNET" 2-3, (ed. 1st 2014).

[4] *Ibid.*

the entire work-life schedule of most individuals has started revolving around the "online" mode.

Data is a valuable resource for every person, company or state. Access to data helps to make informed decisions. Information may be either stand-alone entity information, such as the financial details of clients' access to banking institutions, or at the community level, such as data generated by capturing and processing traffic movement information at an intersection or data generated by climatic conditions or the data gathered during e-commerce usage regarding consumer preferences. Data can be used for analytical, statistical, business and security purposes. The unprecedented explosion in the volume of data creates as much a threat to its misuse as it creates opportunities for utilisation for policymaking.[5]

With the world becoming more digitally sophisticated, even the crimes are becoming complicated to decipher. Everybody is affected by cyber law in some of the other forms, such as almost all companies depend on computer networks to store valuable data. Cyber laws encompass a wide spectrum of issues containing a set of legal aspects relating to internet usage such as data protection, freedom of speech, censorship, intellectual property, software and open-source licenses, unauthorised access, etc.

The Government, too, is resorting to more and more electronic mediums to carry out its day-to-day work. Debit cards and credit cards are being increasingly used for shopping. Traditional law has various limitations when it comes to dealing with cybercrimes. There exist no graphical boundaries in cyberspace. Laws such as the Indian Penal Code, 1860 provide for both territorial and extraterritorial jurisdiction, but the jurisdiction is confined to offences committed by Indian citizens. This leaves confusion as cybercrime has a transnational element. Crimes over cyberspace involve intangible objects, for example, trespass requires an actual physical entry for conviction, but in the case of cyber trespass, no encroachment in the physical territory occurs.

Next is the issue of the gathering of evidence and the monitoring of the crime. There are huge volumes of data involved with the scene of the crime being completely virtual, and also the object of the crime, i.e. information can be easily modified. Legislation is also required in the aspect of surveillance done by companies and government bodies or agencies through data linked identity cards, usage of drone technology etc. There is a lack of transparency and no legal recourse for those whose information is being misused or whose rights are being violated.

[5] *Draft National e-commerce policy,* https://dipp.gov.in › DraftNational_e-commerce_Policy_23February2019 (Nov 2, 2019)

Moreover, awareness about the remedies is negligible among the masses.

III. Relationship between human rights and IT

Technology equipped machines and mechanisms such as mobile phones, social media, and other such tools of mass communication are now central to mobilisation, advocacy and sharing of information and knowledge. They are being used to capture incidents of abuse; more compelling empirical evidence is being provided; satellite imagery can help in cost-effective observance of new dimensions and details of events and objects, and consequently, the efforts and capacities of human rights advocates are being amplified. However, all challenges associated with monitoring and analysis cannot be solved through technology.

Increased volumes of data and more participation of the masses are two broad contributions of technology to the domain of human rights. Digital photographs from space have the potential to corroborate stories on the ground, for example, with land movements suggesting mass graves, deforestation and waste or property destruction. However, using such data is quite challenging. Technology opens up tremendous possibilities for the strategic presentation of information. Websites and online archives offer centralised and expansive repositories for data. For example, Witness and YouTube have created a forum for curating human rights footage from around the world. Another innovative project developed by the New Zealand office of Amnesty International used data mining tools to create an interactive website to demonstrate to the world that any person can be targeted for abuse in a repressive context based on information they voluntarily reveal about themselves.[6]

Technology is not a self-organising platform. It is difficult to assess the impact of the technology specifically. Whenever internet services companies face demands from governments to remove, block or filter content, there is a risk that the human rights of freedom of expression and assembly may be violated. This confers certain responsibilities on companies to respect these rights, often carried out through voluntary self-regulation of illegal content to maintain the openness of online communication. The challenge is to clearly define such responses with transparency, accountability and in accordance with existing laws in order to uphold the procedural rights of internet users accused of violating the law.

Cybercrime legislation defines appropriate conduct requirements for the information and technology sector consumers, which is ultimately acting as a safeguard to human rights. Socio-legal penalties for cybercrime are created through IT laws, and in general, harm to people,

[6] Amnesty International, *TrialbyTimeline*:http://www.trialbytimeline.org.nz/.

software, devices, services and infrastructure is avoided. Inherent human rights such as the right to information, privacy, non-discrimination are involved when through cyber legislation, the investigation and prosecution of crimes committed online are facilitated, and countries cooperate on cybercrime matters.[7] IT laws include rules and standards of conduct for the use of the Internet, computers and such other digital technologies and the activities of media, governmental and private organisations; the rules of evidence and criminal proceedings and other aspects of criminal justice in cyberspace; and policies so that in case of occurrence of cybercrime, the risk or the harm can be reduced to persons, organisations, online networks and infrastructure.[8]

It is pertinent that an illegal act is clearly described in and prohibited by law. If, at the time the person committed the act, it was not prohibited by law, the person cannot be convicted for the same. Technology by itself is never a controversial issue, but what is significant is for whom and at what cost the issue has been in the ambit of the Government. In contrast to the earlier technologies, which had a trickle-down effect, the cyber revolution holds the promise of reaching the masses quickly. This pledge and opportunity can only be achieved with a suitable legal regime based on a given socio-economic matrix.

IV. Issues with substantive, procedural and preventive IT laws[9]

The Internet-enabled digital technologies have facilitated traditional offline crimes such as money laundering, organised theft, forgery and fraud, which are Cyber-enabled, as well as the new world "cyber dependent" crimes. Due to these reasons, many countries such as Germany, Japan, a few African countries and China have amended suitable provisions of their criminal code, and relevant laws have been specifically designed to deal with the traditional as well as the modern aspects of cybercrime. Existing laws are also being used to target cybercriminals. In Iraq, the existing penal code[10] and civil code[11] are being used to prosecute the real-world crimes created through the Internet and digital technology.

(i) Substantive law takes into consideration the guilty act as well as the mental element. The different States have different parameters of what constitutes a crime. The level of criminal culpability with respect to the state of mind varies, and therefore substantial laws are not uniform between countries. Many minor Internet-based

[7] UNODC, https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html, 52.

[8] Ibid.

[9] Ibid, 18.

[10]Iraqi Penal Code No. 111 of 1969.

[11] Iraqi Civil Code No. 40 of 1951.

crimes, which constitute a major bulk of the cyber crimes, are often ignored as they are minimis non curat lex and often ignored although their impact may be substantial collectively.

(ii) Procedural cybercrime law includes rules of evidence and criminal procedure and also provisions on jurisdiction and investigation. Cybercrime having such a huge domain and pervading worldwide, cannot be encompassed within the definite boundaries of a particular country. Therefore jurisdiction poses a major problem in the regulation of such crimes through state laws. The non-existence of geographical boundaries raises questions of the nationality of the criminal and the interests of the parties affected.

When it comes to investigation, digital evidence proves challenging in its handling as well as use in court proceedings. The authenticity of the digital evidence, questions of admissibility, variability in interpretation is another major issue. Apart from this, if the legislation grants highly discretionary and unrestricted power to the authorities, it may pose a big threat to human rights. The cybercrimes act of 2015 in Tanzania provided excess unrestrained powers of investigation in cybercrime to the police. Another example can be cited of Turkey, which is 2014 amended their Internet law 5651 where the Internet service providers were required to make available user data to the authorities without the requirement of first obtaining a court order. Such examples raise deep concern if the powers and procedures are not as per the rule of law, which is one of the most important requirements of today's modern society and human rights.[12]

(iii) Preventive cybercrime law focuses on preventing crime or, at the very least, strives to lessen the damage that may result from the commission of cybercrime. Laws mandating telecommunication service providers to maintain the necessary infrastructure to enable data preservation is an example of preventive law, which is designed in such a way that in the case should cybercrime occur, vulnerability can be minimised. Another example can be of drafting suitable legislation that allows governments agencies to access communications from the service providers with appropriate and lawful authorisation When reliable complaints of the existence of any exigencies have been reported. Unfortunately, hardly much legislation in this domain exists worldwide, with a few exceptions such as the European Union

[12] Article 15, The Council of Europe's Convention on Cybercrime of 2001.

General Data Protection Regulation of 2016, The Cyber Law of Ukraine[13] and The Communications Assistance For Law Enforcement Act of 1994 in the US. The biggest issue with preventive legislation is that the law-making body or the government authorities may use such laws In a wrongful manner in order to advance their own interests having little consideration for the original purpose of the legislation.

V. The intersection of IT laws and human rights

Provisions of various cybercrime laws, especially the Internet-related ones, for example, the laws related to defamation of the head of the state, obscenity or pornographic material, disrespect for authority, along with the provisions that lay down how their tools should be used during the investigation of cybercrime facilitating the interception of communications and electronic surveillance may justifiably restrict the exercise of certain human rights. Therefore there is an urgent need for a balance between the control of cybercrime through state means of legislation and respect for human rights.

An important role is played by the world community in the enactment of human rights through the International human rights law. However, these laws are much affected by the national legislation, and vague and overbroad justifications such as references to national security, public safety, protection of morality, economic and health security or terrorism in the IT legislation often dilute aspects of the fundamental rights of the man. Restrictions should only be authorised when they pursue a legitimate aim and are necessary and proportionate to the threat that justifies their implementation. But since IT laws are still at such a nascent stage, it intrudes upon human rights often without the actual intention of violation.

(A) Freedom Of Speech, Expression And Information

One of the most precious rights of man is the free communication of thoughts and expressions.[14] This right includes the freedom to hold any opinion without interference and seek, receive and distribute information and ideas through ‘any’ media, irrespective of borders.[15] Thus, such rights are equally applicable to the cyber world. An individual and the community alike should have the liberty to articulate opinions and ideas freely with no fear of suppression, sanction or stringent action. However, the rapid growth of social media has seen an unprecedented increase in cases and instances of fake information, misguided ideas and hate

[13] The Basic Principles Of Ensuring Cyber Security Of Ukraine Of 2017.

[14] Article 11, The Declaration of the Rights of Man and of the Citizen.

[15] Article 19, The Universal Declaration of Human Rights, 1948.

speeches. Common and reasonable limitations are therefore imperative. But the problem arises when on the one hand, government authorities may exceed their controlling actions, consequently violating the freedom of speech, thoughts and expression. At the same time, in the name of human rights, individuals, communities and organisations are often seen misusing the freedom bestowed upon them by committing acts of libel, disseminating fake information, resorting to obscenity, committing perjury, sedition, or copyright violations.

(B) Data privacy and security

The creation of a nationwide identity system is one proposal that has been received as a solution for problems ranging from counterterrorism and detecting fraud to preventing illegal immigration and also enabling electoral reforms. This digital ID system has been challenged on constitutional privacy grounds. Their introduction has also seen a range of unforeseen administrative and social complexities in recent times. Every identity system, like ID passport, Visa is made up of a support register containing personal information. The new development of biometric technology in the national identity system can be said to amount to a wholesome violation of human rights, especially to the rights to privacy and thus cannot be justified on the grounds of national interests. But what remains challenging is to ensure that this information is used judiciously only for the ends of justice and is not subject to manipulations and undue wrongful usage.

In the case of social media, social networking sites are the tools to coordinate opinions from different people from various parts of the world. It is being immensely used to promote human rights such as the freedom of expression and opinion and the freedom to assemble peacefully. But often, these rights have been misused, resulting in violation of privacy, defamation, assault, libel and many more other wrongs. The case of the Israeli ‘Pegasus’ software being misused by officials is a glaring example of gross invasion of individual and national privacy.

(C) Lack of Transparency- Intended and Unintended use and misuse of ICT and IT laws

Technology is increasingly being used by governments to surveil and censor their citizens both legally and illegally. The infrastructure that is owned by private actors such as transnational and national companies also exert much control over private user information. There have been frequent instances where the private companies and the corporate sector have sided with the governments who have used the digital infrastructure and the network in ways that cater to their interests, the underlying effect of which is often a direct violation of individuals’ rights to privacy, free expression and freedom of association. This can further create a chain of online violations. A case in point is the recent Facebook Cambridge Analytica data scandal. The prosecution of a Chinese journalist[16] was also much in the news when it was revealed that Yahoo! China had revealed his details to the Chinese Government for revealing details against the latter.

Not enough rules govern private companies as well, who have access to unprecedented control over online content, and this vulnerable data can be sold to sell people into shams and scams.

(D) Lackadaisical framework

There does not exist a similar and cohesive flow of legal provisions across the borders. Moreover, IT laws are either absent or plagued with the lacunae of not being updated with the latest development in the information technology area in most areas of the world. Even highly advanced countries such as the United States of America report one of the highest percentages of cybercrimes.[17] The IT Act overlaps with the aspect of human rights, as can be seen from the recent scrapping of Section 66A of the Act. Even the recently introduced The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, have been hugely debated.

(E) Internet censorship laws

Internet censorship is the regulation and restriction of what can be downloaded, posted and viewed on the Internet by authorities or on their own initiative.[18] Censorship in many countries has become an instrument through which the speech and views on cyberspace have been regulated by the Government. Numerous reports[19] have been released which have documented how Internet speech is filtered across various countries. A glaring example is China, followed by Singapore, Iran, Saudi Arabia, as well as countries like the US and India, which have engaged in similar practices of Internet censorship. Such examples of perpetration raise many underlying questions as to whether the government authorities have a legitimate role in controlling and limiting access to information and to what extent and what form such regulations are acceptable.

The Chinese Government, as a measure of information control, resorted to forwarding requests to the Google search engine to its own search engines, which were controlled by the state. In 2011, when the Arab Spring took place, the media played an extensive role with social

[16] *Joseph Kahn ,Yahoo helped Chinese to prosecute journalist,* http://www.hrw.org/news/2009/10/11/banned-censored-harassed-and-jailed *(Sept 8, 2005).*
[17] *supra,* note 8
[18] Schmidt, Eric E.*;* Cohen, Jared . *"The Future of Internet Freedom*". New York Times *(Mar 1, 2014).*
[19] "Open Net Initiative.

networking sites availed through the use of mobile and Internet technologies to organise, spread and bring to light the protests to the rest of the world. The subsequent response in countries like Egypt, Libya and Syria was the imposition and increase in censorship as well as complete loss to the access to the Internet for prolonged periods of time with blocking of sites, putting sanctions and taking vigilante actions against the slightest hints of defiance. Censorship has been resorted to time and again in different magnitudes raising a huge question on the freedom of the people. In the Kashmir Valley, following the abrogation of a clause of article 370, internet access was completely shut down.

(F) Public Privacy and Surveillance

The increasing installation of CCTV cameras in public places has ushered in a new mass surveillance system. This form of public surveillance has the advantages of 1) ensuring faster and efficient investigation of crimes, 2) deterring crimes due to the threat of being caught more easily 3) ensuring safety to the public due to lessened susceptibility of wrongdoings in the presence of a recording device. The crime rates in many places have substantially dropped after the surveillance systems have been set up. Evidence and clues can be gathered more easily.

However, there are concerns with respect to issues of a reasonable expectation of the right to privacy and its abuse. There is a dearth of laws regarding the installation of CCTV cameras, with regular incidences of hidden cameras in private areas such as changing rooms, bathrooms and hotel rooms being brought fore. Apart from this, the footage is sometimes used to commit acts of blackmail and even voyeurism.

Drone technology is an advanced form of surveillance mechanism initially thought of as an item of weaponry, but today, drone technologies, such as video cameras that can record audio and video content, threaten the right of individuals to privacy. In the recent past, countries, including India,[20] have been coming up with rules and laws on drone usage, but much work still remains to be done in this area.

(G) Crimes affecting Women and Children in particular

Abuse of rights online can enable abuse offline. The free flow of information in the cyber world and also the way in which people are encouraged to lay down their everyday details so explicitly for the world to see has created more problems of cyber harassment, cybersquatting, cyber pornography, cyber defamation, morphing, email spoofing[21], child trafficking,

[20] Press Information Bureau Government of India Ministry of Civil Aviation 27-August-2018 19:37 IST Government announces Regulations for Drones Regulations will be effective from 1stDecember, 2018 Operations of Remotely Piloted Aircraft System (RPAS) to be enabled through Digital Sky Platform

[21] Rajat Mishra, "*Cyber Crime Against Women*" https://ssrn.com/abstract=2486125 or

cyberbullying and identity theft.

While online women rights movements such as #MeToo[22] shook the world around, there is a rising question on the frail women laws across countries in the patriarchal society, especially after instances of cyber abuse reporting has seen a tremendous rise. Technology in the hands of vulnerable children, along with a much ignorant and naive society, can be manipulated by criminals and software applications on smartphones have been proved to be fatal in the rightful growth of the next youth. Sexual predators regularly put out a lot of videos on social media sites that target children and teenagers, grooming and coaxing them into sexual acts and fraudulent behaviour.[23] A case can be cited of TikTok, a Chinese mobile app that allows child selfie videos to become so accessible that their quest of being a social influencer and false peer pressure can lure them into extreme measures and even sexual abuse rackets. It was temporarily banned in India as well, but the repercussions to it were hidden due to the lack of adequate evidence of the extent of influence.[24] The Blue Whale Challenge[25] was another online suicide game that raised international concerns on the invasion and needs for regulation of the aftermaths of wrong use of IT.

(H) IPR violations

A person has the right to protect the moral and material interests arising from his work, and this is a fundamental human right.[26]Various national and international laws and treaties that have been developed specifically for intellectual property govern the protection and enforcement of intellectual property rights. The easy access to online sources has led to an increase in online copyright infringement. Cyberspace unique trademark infringement constitutes cybersquatting, the use of trademarks in a meta tag, keyword infringement, reverse domain name hijacking etc. Bad fate is an important component to detect whether intellectual property violations have been carried out. The indigenous community's rights are especially at risk when the flaws in the IPR laws and their misuse lead to exploitation and infringe on the domain of the human rights law.

http://dx.doi.org/10.2139/ssrn.2486125

[22] Indulekha Aravind, A year since #MeToo: What has been done is #TooLittle, available at: https://economictimes.indiatimes.com/news/company/corporate-trends/a-year-since-metoo-what-has-been-done-is-toolittle/articleshow/71456710.cms?from=mdr

[23] Venkatesh Ganesh and Jinoy Jose P, Our kids are not safe online, available at: https://www.thehindubusinessline.com/specials/india-file/our-kids-are-not-safe-online/article26501956.ece

[24] *Ibid*

[25] Gemma Mullin, CHILLING CHALLENGE What is the Blue Whale suicide game and how many deaths are linked to the challenge?, available at: https://www.thesun.co.uk/news/worldnews/3003805/blue-whale-suicide-game-challenge-deaths-uk/

[26] Article 27(2)(i). Universal Declaration Of Human Rights, 1948

(I) Right To Be Forgotten

The right to be forgotten is the claim of an individual to have certain data away from the reach of third persons and the right to silence past events in life that are no longer occurring.[27] Internet records delete their information to maintain their privacy on certain grounds. There are few protections against the harm that incidents such as revenge porn sharing, or pictures uploaded due to poor judgement, can do.

(J) E-commerce Policies

In the age of e-commerce, companies have come to have access to large amounts of data of individuals. A pertinent issue that arises here is whether the company has any right to this data, especially if it decides to exploit it. Would an individual be expected to pay the company for access to his own data? Would a Government be willing to pay private corporations for data about its citizens?

(K) Digital currencies

The advent of cryptocurrencies such as Ethereum and bitcoins has created a vast hidden financial market in the digital world outside the purview of official monitoring. Online gambling, laundering and financial frauds are a few of the many repercussions of their use. This raises a lot of questions on the need for their regulation, with many Governments now in the process of drafting suitable legislations to decide their legality or considering issuing their own form of digital currency.

VI. Conclusion

A myriad of new technological opportunities is available in the human rights ecosystem today. The modern-day human rights movement is interwoven by technology which is foundational and permeates all areas. Information combined with technology has opened up enormous opportunities for the advancement of human rights efforts, but there is also a growing need to safeguard and provide security to not just human rights defenders and activists but the everyday citizens as a whole in today's world globalised surveillance.

In a world where the boundaries between physical and digital space are increasingly getting obscured, it is pertinent to understand the technological, legal and political infrastructure that affects the rights in the digital sphere to ensure that basic human rights are upheld. With the growing information technology scenario, it has become ever the more important and urgent

[27] PINO, G., THE RIGHT TO PERSONAL IDENTITY IN ITALIAN PRIVATE LAW: CONSTITUTIONAL INTERPRETATION AND JUDGE-MADE RIGHTS- THE HARMONIZATION OF PRIVATE LAW IN EUROPE 225-237(1st ed. Oxford: Hart Publishing, 2000)

that the violators of rights in the physical world and online are held accountable and monitored so that the capacity of the human rights movement can be enhanced. This again calls for an important role played by technology to monitor and build evidence of abusers, as well as the promotion of policies for infrastructure development to protect basic liberties. Thus IT Laws need to be used as a tool to make human rights more efficient and secure.

IT-related crime is an international issue. Today a majority of the countries worldwide have domestic laws that cover some or the other facet of cybercrime, but in countries where cybercrime laws still do not exist or are weak, safe cybercrime havens are created, and the person cannot be prosecuted unless the law considers the activity to be illicit enough to be punishable. In 2014, the Philippines did not have a cybercrime law, and the "LOVE BUG"[28] computer virus created and distributed by a resident of the country could not be prosecuted, although this virus had immense adverse economic consequences all around the world. Through harmonisation, not only can cybercrime be adequately addressed, but also international cooperation will be facilitated. Digital evidence and forensics data of one country, if admissible in other countries, would aid cybercrime investigation and the redressal mechanism. In 2015, Nigeria drafted the law to establish a Cyber Crime Advisory Council that could facilitate international cooperation on matters dealing with cybercrime. A national and international database such as the United Nations Office on Drugs and Crime Cyber Crime Repository of laws on cybercrime and the case laws would go a long way to strengthen the impact of IT laws worldwide.

Artificial intelligence, big data analytics and blockchain technology altogether have been shaping our future. In such a scenario, the need is to come up with an approach where the legal provisions are drafted keeping in mind the human rights approach and the methodologies followed are such that freedom of expression, information, right to privacy and other basic inherent rights are built-in from the start. Miscellaneous laws such as those dealing with health care, education and financial services also need to imbibe the realisation of human rights to improve the transparency and the responsiveness to the Justice system. Innovative technologies such as photo DNA, the use of biometrics and big data analytics can be used by governments, companies and human rights organisations more beneficially if they are governed by adequate legislative benchmarks.

The networking of objects, devices, people, and organisations to create the so-called "internet of things" is enabling a wide range of new products, services, and solutions, such as smart

[28] https://www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html

cities, sustainable agriculture, self-driving cars, connected healthcare, and more efficient industrial processes. These opportunities are accompanied by new risks and challenges, such as the difficulty of obtaining informed consent from citizens for data use or the need to establish privacy protocols for who has access to data, who controls data, and how data is used. These challenges form an important new social license to operate—without public trust, the Internet of Things is much less likely to become a commercial success.

UDHR calls for the protection of free expression in all forms of media[29] , including rights such as freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of boundaries and frontiers[30]. Freedoms of expression, association, information and also the rights to privacy depend even more on the significance that infrastructure adds to safeguard human rights and also on various security tools to help individuals control access to their information.[31]Instances of hate speech have to be curbed by suitable legislative and administrative actions.

i. Digital rights concept

Issues include overarching concerns of developing, monitoring, and advocating for rights and freedoms in the digital networked sphere, as well as privacy-enhancing tools that add layers of security around the technologies that activists and citizens use in their daily work online and via mobile telecommunication networks. Governments are increasingly interested in proactive monitoring, surveillance, removing, and blocking certain types of content, especially terrorist content and hate speech. These content restrictions are important for human rights protection but must be "necessary and proportionate" and the least intrusive restrictions to achieve the desired result.

Access to appeal and remedy in the event of over-blocking is crucial. Companies face the risk that law enforcement agencies themselves violate human rights, such as when surveillance powers are misused, overbroad requests for data or content restrictions are made, or governments make use of hacking techniques without proper approvals. Transparency about company relationships with law enforcement agencies (including sales relationships) is increasingly important.

An Individual owns the right to his data. Therefore, if at all the data of an individual is used, it must be with his/ her express consent. This consent has to be expressed in a form

[29] Article 9, UDHR, 1948

[30] Ibid

[31] PRIMA TECH REPORT

understandable and regarding the uses to which it shall be put.[32]The Internet has now been globally recognised as a fundamental right in order to exercise and enjoy their rights to freedom of expression and opinion and other basic human rights. This right has been curbed around the world in curfews and mass government actions.[33]

ii. Addressing the data issue

Challenges include the sheer volume of both content data and transactional traffic data, the fact that data is perpetually in motion and the specificity of the data. There is a need for people to secure data that contains identities, locations, and personal information. This extends to the people who are using tools for human rights documentation, to victims and witnesses being documented, and even to the families and friends of human rights defenders. The risk also expands beyond targeted subjects, as online surveillance can uncover almost any individual's location, trace their communications, and divulge the identity of their associates. The broad challenge is to provide end-to-end encryption in a user-friendly manner to non-technical users. While data may be lawfully intercepted and retained by law enforcement agencies, protection of individual privacy and data security must be paramount.

Strong encryption (i.e. authentication of digital interactions) is increasingly accessible for everyday communications, such as email, voice, messaging, and cloud storage. Encryption provides the privacy and security necessary to exercise the right to freedom of opinion and expression in the digital age and is especially important for human rights defenders, vulnerable populations, and whistleblowers. However, law enforcement and intelligence services are concerned that encryption makes fighting crime (e.g. drugs, terrorism, and fraud) tougher, and they are using public policies or hacking techniques to prohibit and fight it. Some states are implementing or proposing "back doors" to get around encryption—but providing "special access" to government authorities can weaken everyone's online security and privacy.

"Technology is not the subject. Technology can be instrumental and transformative, but 'what we do with technology to advance our social and human rights goals is the keyframing."[34] Several international treaties have been implemented relating to cybercrime. Overall, existing multilateral and regional legal instruments and national laws vary in terms of thematic content

[32] Draft e commerce policy

[33] IS INTERNET ACCESS A HUMAN RIGHT? Avaible at: https://www.amnestyusa.org › is-internet-access-a-human-right

[34]Tamy Guberek and Romesh Silva, Human Rights and Technology: Mapping the Landscape to Support Grantmaking, available at: https://www.academia.edu/25810320/HumanRights_and_Technology_Mapping_the_Landscapeto_Support_Grantmaking

and extent of coverage of criminalisation, investigative measures and powers, digital evidence, regulation and risk, and jurisdiction and international cooperation. These treaties also vary in geographic scope (i.e., regional or multilateral) and applicability. This variation creates obstacles to the effective identification, investigation and prosecution of cybercriminals and the prevention of cybercrime.

Safeguards are needed to ensure that laws that place restrictions on Internet access and content are not abused and are according to the rule of law. The clarity in the law is also needed to ensure that laws are not used to prohibit access to content in a manner that violates human rights law. What is more, challenges concerning the reach and effect of cybercrime laws arise where "Internet content that is generated and acceptable in one country is made available in a third country" where the content is considered illegal.[35]

To sum up, though a crime-free society is perfect and exists only in illusion, it should be a constant attempt of rules to keep the criminalities lowest. Especially in a society that is dependent more and more on technology, crime based on electronic law-breaking are bound to increase, and the lawmakers have to go the extra mile compared to the impostors to keep them at bay. Technology is always a double-edged sword and can be used for both purposes – good and bad. It should be the duty of the three stakeholders viz. i) the rulers, regulators, lawmakers and agents ii) Internet or Network Service Suppliers or banks and other intercessors and iii) the users to take care of information security playing their respective role within the permitted limitations and ensuring obedience with the law of the land.[36]

VII. Suggestions

1. Need for empowered judicial action- The taking up of cyber-related cases within the purview of traditional law requires active vigilance on the part of the judiciary to make sure that adequate remedial action can be provided by clubbing the provisions of older laws and blending them with the current technologically advanced age. Judicial reforms in the cyber domain will go a long way to render speedier justice, especially in cases of cybercrime that require urgent action to track and source the culprit and his actions.
2. A common cyber law platform at the International level- Although a number of agreements and conventions have come up at the international level, there lacks a common platform that can provide uniformity and allow the cyber-related cases to be solved across borders without the conflict of non- similarity of domestic laws across the globe.

[35] (UNODC, 2013, p. 115).

[36] All You Need to Know About Cyber Laws In India file:///C:/Users/User/Desktop/seminar%201/All%20You%20Need%20To%20Know%20About%20Cyber%20Laws%20In%20India%20-%20iPleaders.html

3. Revamp in the existing legislative framework- The IT laws still have been lacking the required enforceability and stringency that shall cater for the increasing number of cases in the information technology area. Also, a number of IT-related aspects have yet not been incorporated in the legal terminology and framework that makes the laws redundant when miscreants get away with the loopholes in the mechanism. National cyber security policy, 2013 has been drafted to exercise a check on the security issues in the cyber network. Child victims of cybercrimes can now lodge their complaints at National Commission for Protection of Child Rights (NCPCR)'s POCSO e-box. These are welcome steps.

4. A separate data repository regulatory body- Apart from the creation of a data repository, there also is the need for an empowered regulatory body to manage the huge amounts of data reserves created. Also, the set up of more cybercrime-related cells and a systematic monitoring body to exercise a check on violations is needed.

5. Investment in technology- including infrastructure and tools, technology itself is rarely the proper subject from which to begin to identify and understand human rights problems and challenges. Thus there is a need to develop the infrastructure that incorporates technology to fight against technology misfeances.

6. Imbibing human rights aspects from the very start of legislative deliberations would be another reformative step to counter the conflict between the Information Technology framework and human rights.

*****