Beyond Briefs Law Review

Volume 1 | Issue 1

2023

This article is brought to you for "free" and "open access" by Beyond Briefs Law Review. It has been accepted for inclusion in Volume 1 Issue 1 of Beyond Briefs Law Review after due review.

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of the Publishing Editor of Beyond Briefs Law Review. The Editorial Team of Beyond Briefs Law Review and the Author holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of Beyond Briefs Law Review. Though all efforts are made to ensure the accuracy and correctness of the information published, Beyond Briefs Law Review shall not be responsible for any errors caused due to oversight or otherwise.

CYBER ETHICS: MODERN CODE OF CONDUCT

~ Sanchita Kushwaha[1]

Abstract

*Society needs a certain balance for its existence. This balance may be grounded in moral conduct and ethical behavior, at different levels. We live in- **the era of social media,** and it has over time become a place where our personal and professional information is often disposed of and stored. Consequently, crimes in cyberspace have become very common. The screens in the cyber realm allow the offender to hide behind them and execute their ill-motives secretly. The government has over time realized the attention that is needed immediately to establish order in cyberspace and has taken certain initiatives. Laws in India, like- **the IPC, 1860; the IT Act, 200; and the DPD Act, 2023,** along with variable rules and guidelines, have been of importance in controlling and punishing cybercrimes. The local/state level authorities have also actively contributed to the elimination of cybercrimes and getting hold of culprits. There follows a long list of **measures** that are to be taken in accordance with the laws, to ensure a society that is well-equipped and protected from cybercrime.*

---

[1] You may contact the author at the following email address: sanchita.kushwaha@gmail.com

INTRODUCTION

A society is governed by certain morals, and these morals govern the functioning of society in-turn. We, as humans, clearly have privileges over other living creatures with whom we share the planet, and consequently, our society is more complex. We can think and act, and all humans possess a variable behavioral pattern, but society considers certain acts to be morally unethical and criticizes them. Today, in the era **of social media**,' we have a huge reach, even to the corners of the world, for good and bad. The things that were once thought out 'out-of-reach for a civilization are now made possible by social media, the internet, and its related mediums. Consequently, this growth that exists in the ambit of human access has resulted in the growth of crime as a backlog. People of all backgrounds an access to internet platforms and mediums, including the hoodwinkers of our society; what else is better to them than having a screen to hide behind from their malicious crimes.

A list of famous philosophers has added to this debate about crime and human psychology. A huge crowd stands in favor of- **Reformation theory**- which believes in the reformation of the offender to establish a better society. whereas others fall in favor of- **Deterrence theory**, which emphasizes punishment and creating a deterrent affect to avoid crimes in society, respectively. Although, their are several other theories, these stand out as the most prominent part of the discussion. Many believe that humans are resistant to crime only when a punishment or any other legal binding lays over them. While others argue that societal pressure also plays a major role, including famous philosophers of- H.L.A. Hart. We may eventually put an end to this debate, in-relation to social media/Internet. Why? Clearly, because the criminals have less of a threat of being exposed to society as they conduct crimes while hiding behind their screens; these screens eliminate the societal pressure and pose a threat to our society for the same reasons.

Some might argue that- even then, when they are caught, they must bear the societal shame, but how often does this happen? The very common and famous instance is the comments on varied posts of public figures; we see certain well-wishers but to add on to it there is a cruel army of trolls, and they spare none. It may sound irrelevant as towhat theyt cay do just bycommenting,g but to not forget how they still cross the ethical line, not in person but in the virtual world, those words still reach thevictim,m tearing apart their dignity and at times causing mental trauma. Just because it happensonh the internet and the wrongdoer is behind ascreen, shall, wl ignore it and move on

with our lives? The best advice we come across for these questions is that-they should be ignored, as they appear harmless, but not forgotten, forget- they exist among us and will over time pollute the whole society, including the tender minds that have access to social media.

Cyber ethics are basically certain mandates that are to be followed by and among the users in an online environment, i.e., basic ethics while making use of cyberspace. These include the basics of being a responsible citizen. Law and related bodies within countries realize the severity of the issue and cyber ethics and have gone to great lengths to establish related laws or legislation.

LEGISLATIONS/ACTIONS INITIATED

The laws that govern Cybercrime in India are:

o **Information and Technology Act, 2000**- The Act goes through the problems of existent regime, like- Hacking,obscenity, Privacy breach; etc. It has sections that discuss and emphasize cybersecurity. Discussing several prominent chapters: **Chapter V**- Secure Electronic record and secure Electronic Signatures; **Chapter VIII**- Duties Subscribers; **Chapter XI**- Offenses, **Chapter IX**- Penalties, Compensation; Adjudication; and **Chapter X**- Appellate Tribunal,bunal; etc. This Act is among the first and very prominent Acts that govern the cyber-sphere.[2]

o **Digital Personal Data Protection Act, 2023**- The Act comes out to be a perfect blend of- data privacy and protection and accessing data for legal purposes.. The Act emphasizes on- **consent** (Section 6) of the data principal along with the inclusion of- **Processing of personal data,applicability; Rights and duties of data principal, Obligation of data fiduciary ; Data transfer penalties,** etc The case is to be taken to- Telecommunication Dispute Settlement and Appellate Tribunal **(TDSAT)**, established under **TRAI** Ac1997.[3]

o **Indian Penal Code, 1860**- IPC has also been very specific and evident, while emphasizing matters of cyberimportance. .We were, discussing several sections: **Section 378- Theft**, including 'movable property' may also be regarded in term of- any data, online or otherwise; It includes all sought of corporeal properties and any offense here is punishable by imprisonment up to 3 years or fine or both. **Section 424- Dishonest or fraudulent**

---

[2]Ministry of electronics and information technology, Govt. of India, https://www.meity.gov.in/content/cyber-laws
[3] Ishwar Ahuja and Sakina Kapadia, 'Digital Persona; Data Protection Act, 2023', Bar and Bench, 22 August, 2023,https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis

removal or concealment of property, this includes Data theft is punishable by imprisonment for up to 2 years, a fine, or both. **Section 425- Mischief**, involves mischiefs conducted on or through computer systems and is punishable with imprisonment up to 3 months, a fine, or both. [4]

o **National Cybercrime Reporting Portal**- The portal was launched in 2019. This was launched to provide public with a platform to place their complaints relating to cybercrimes; majorlya major emphasising on the crimes like-child sexual abuse or child pornography, gang rape imageries and other sexually explicit content. **Indian Cyber Crime Cordination Center** were also launched to monitor any offensive activities on media platforms. Also, the Cyber security related incidents are to be reported to- **CERT**. The govt. has made other centers as well to monitor o avoid any such offences- Cyber Swachhta Kendra; etc.[5]

Many state and district-level authorities have also taken **initiatives** in the related sphere:

o The **Police Commissioner of Hubballi** has initiated conducting visits of school/college children to the Police Commissioner's office; the authorities are aware of the young age group being the majority population on social media and have considered making them aware of the **cybercrimes- on ways to avoid/eliminate them, and giving them first-hand information**. Here, the very recent visit included a group of 60 students.[6]

o **Uttar Pradesh has** in recent times witnessed the second position in relation to the conduct of cybercrimes, with a total of **3 Lakh crimes** in the last three-year span. **Prof. Triveni Singh** discusses how youngsters are being fooled by such offenders online. These crimes are being executed by apps like- OLX and other third-party applications. He points out on the **measure** to avoid such crimes is to avoid the application of Third- party applications, like-Anydesk; etc. and advices youth to be more alert; Other authorities in variable states

---

[4] Vinod Joseph and Deeya Ray, Cybercrimes under the IPC and IT Act- An uneasy co-existence', Mondaq, 10 February,2020,https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act---an-uneasy-co-existence

[5] , 'Steps taken to deal with cybercrime and cyber security 'Press Information Bureau, Govt. of India, 17 July, 2019, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1579226

[6] Basavaraj Kattimani, 'Police commissioner takes special measures to deal with cybercrimes', The Times of India,18August,2023,   https://timesofindia.indiatimes.com/city/hubballi/police-commissionerate-takes-special-measures-to-deal-with-online-crimes/articleshow/102818359.cms

have mostly been observant and active at their levels. [7]Also, the UP police has initiated-
Digital Literacy Programmes as well, to educate the general public within the 8 Districts of Agra in order to efficiently dissolve cyber complaints. [8]

ACTIVITIES

Considering several activities that fall within the ambit of **cybercrime types** are:

o   Keeping or sharing videos videos/images that may be obscene or indecent and harm the dignity of others, or conducting activities relating to child sexual abuse and presenting the related material online. (Child sexually abusive material)

o   Abusing or harassing by any means using the online medium/internet. (cyberbullying)

o   Stalking someone by means of-chats or mails or social media posts; etc. (Cyber Stalking)

o   Deceive people with fake pretentious behaviors (Phishing and Vishing), etc.[9]

Other forms of cybercrime may include: Hacking or spreading virus in systems, Making use of property or any kind of internet service without the knowledge of owner; etc. These may include monetary or non-monetary crimes. And, being a reasonable person, one must avoid such behavior and opt for the appropriate and proposed conduct- ethics.

ISSUES INVOLVED IN CYBERCRIME

Cybercrimes have arisen so widely in recent times that there existence, even in the virtual world, is as real as ours. Cybercrimes, when conducted, take variable forms and involve some serious issues of societal importance:

o   **Harassment-** Children these days are introduced to social media at a very tender age and are harassed consequently, as they are very young to possess a sense of compassion and often get involved in rivalries causing wrong. As per a report, India faces the highest percentage of harassment or cyberbullying (37) among children as informed by parents.

---

[7] HT Correspondent, Cybercrime: 3Lakh cases reported in UP in 3 years, Hindustan Times, 10 November, 2022,https://www.hindustantimes.com/cities/others/cyber-crime-three-lakh-cases-reported-in-u-p-in-three-years-101668018847283.html
[8] Amil Bhatnagar, UP cops carry out- Digital Literacy Drive for Cybercrime, Indian Express, 27 June, 2021, https://indianexpress.com/article/india/up-cops-carry-out-digital-literacy-drive-for-cybercrimes-7378004/
[9] Nikunj Arora, Cyber Crime laws in India, Ipleaders,28 April, 2022, https://blog.ipleaders.in/cyber-crime-laws-in-india/

Not just children, but even adults up to 40%—face anxiety and stress due to cyberbullying. [10]

- o **Privacy breach-**A data leak for many may be of no news buto some, it may cause an impact of an accident. An article discussing the same through light on related incidents and consequences in the Journal of Medical Ethics by Stanford professor of psychiatry and behavioral sciences discuss- patients going through traumas and anxiety issues due to leakage of their personal details. s.[11]

- o **Security breach-** Security plays a major role in harmonious societies across the globe but it may be under threat due to cybercrime- The ransomware attack that was projected on Delhi AIIMS in 2022 pointed on the existent holes in the cybersecurity set-up; The AIIMS attack was linked with-Chinese links. CERT observed a increased number of incidents from 2020 to 2021, by 21%. [12]Although, several guidelines are being introduced, by the emphasis on there execution should be the point-of-attention.

There is a list of other related issues, but these stand out as pioneering. The laws of the country along with the respected authorities have been trying lately, to reduce these cybercrimes through variable initiatives, and it won't be wrong to say that, we shall also act as responsible citizens and follow the laws or guidelines, along with opting for certain measures.

MEASURES

Cybersecurity is not easy, but it comes down to three basic Principles- Protect, detect, and Respond- NIST, US Department of Commerce). These principles are the basics, although they exist in other countries organizations. Their adaptation may serve as a boon, and in order to be embodied, they are executed via several measures.

- o **Education-** An educated and aware society is the one that avoids crime efficiently. Children at school level should be taught about these crimes and its consequences, to build a prosperous society, E.g., Introduction of subjects that particularly aim on cybercrimes

---

[10] Same Cook, Cyber bullying facts and statistics 2018-2023, Comparitech, June 19 2023 https://www.comparitech.com/internet-providers/cyberbullying-statistics/

[11] Ray Walsh, Data Privacy: Is it a mental health issue? Proprivacy, 5 June 2019 https://proprivacy.com/privacy-news/data-privacy-mental-health-concern

[12] Anupriya Chatterjee, India's had the worst year in cyber-attacks but2023 will see govt. And firms ramp up defence, The Print, 30th December 2022, https://theprint.in/india/indias-had-its-worst-year-of-cyberattacks-but-2023-will-see-govt-firms-ramp-up-defences/1286441/

and related safety because these tender minds constitute to form the major online population; etc.

o **Workshops-** Practice and exposure enhances our knowledge. Schools and other educational organizations should arrange related workshops where people are encouraged of cyber safety and ways to be cautious for i.. These workshops may be held in institutions as well as local areas like- Schools/colleges, community parks, cafes; etc.

o **Awareness/Precautions**- People should be informed through mails or call or advertisements on 'How to detect and avoid cyber-Fraud.' The measures may be- Setting up strong and different passwords, not sharing confidential information frequently with anyone, installing firewalls; etc.

o **Keeping Checks-** To look for any suspicious activities around or on system/software, as-precautionn is always better than cure.

o **Help-** Reaching out for help, even after executing the adequate measures or due to any casualty, removes the stigma around cybercrimes, which majorly involves- **'victim blaming,'** i.e., individuals shall not be discouraged to use media platforms in incidents, but rather encouraged when they come-out against such crimes.

After the Corona times, things have been different and way more digital than we could have thought. The workplace has shifted from manual to virtual means, and so has the database. A lot of information goes through and is stored on computers today, many of which are highly confidential in nature, and consequently, there is an enhanced need for settling lines and precautionary rules to be placed to avoid crime in the cyber realm. In a recent incident-A cybercrime was observed in India and was rooted in Dubai. The crime observed money extortion from individuals across the country by impersonating- NCB, CBI, ED, Police officer; etc. and consequently, 17 branches have been frozen.[13]

Not to forget that, the generation of today lives on the internet and does many activities online. They are often negligent, which at times causes havoc. They are to be aware and cautious of the potential threats they have, how can be secure and what activities falls within the category of cybercrime, even in situations when they are unaware- Cyber Ethics allows to facilitate the

---

[13] OEO wings unearth huge cyber fraud with roots in Dubai, The Telegraph Online, June 26, 2023
https://www.telegraphindia.com/india/odishas-economic-offences-wing-unearth-huge-cyber-fraud-with-roots-in-dubai/cid/1947629

same and we are the ones responsible for this safe and secure environment. ***"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace.''-*** **Sir Newton Lee.**[14]

---

[14] Newton Lee>Quotes >Quotable quotes, good reads,https://www.goodreads.com/quotes/789592-as-the-world-is-increasingly-interconnected-everyone-shares-the-responsibility