INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 1 [2025] | Page 488 – 514

THE IMPACT OF CYBERCRIME ON HUMAN RIGHTS

-Dr. Swarupa Dholam [1]

-Miss. Aditi Sawant[2]

ABSTRACT

The rapid advancement of digital technologies has led to a significant rise in cybercrime, posing critical threats to fundamental human rights. This research explores the intersection of cybercrime and human rights, focusing on how various cyber offenses—such as hacking, cyberbullying, identity theft, digital fraud, and surveillance—violate individuals' rights to privacy, freedom of expression, and security. It highlights key legal frameworks, including India's Information Technology Act and international conventions, while analyzing landmark judicial precedents that shape digital rights.

The study also examines public perception through survey-based data analysis, revealing gaps in awareness, legislative enforcement, and digital literacy. Findings suggest that while existing legal mechanisms attempt to regulate cybercrime, there remains a pressing need for a robust data protection law, cybersecurity awareness programs, and global cooperation in cyber law enforcement. The research concludes with recommendations for policymakers to balance digital innovation with human rights protection, ensuring a safer cyberspace for all.

INTRODUCTION

How does the cyber crime overshadow the human rights? Why don't the law makers take cognizance of the violations of human rights as enshrined in the universal declaration of human rights? Answering all these questions need to be researched along with the efforts made by the government and social organisations, institutions and also individuals.

Cyber space can be defined as an intricate environment that involves interactions between people, software and services.

[1] Dr. Swarupa Dholam presently serving as Registrar of Maharashtra State Human Rights Commission, Mumbai deputed from the cadre of Civil Judge Senior Division, of Maharashtra Judiciary Services.

2 Miss. Aditi Sawant is Law student of National Law University, Nagpur

- The views expressed are those of the authors alone.

Cyber security denotes the technologies and procedures intended to safeguard computers, networks and data from unlawful admittance weaknesses and attacks transported through the internet by cyber delinquents.

Cybercrime is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

The Ministry of Electronics and Information Technology under the Government of India provides a strategy outline called 'The National Cyber Security Policy' in 2013. The main intention of the said policy is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

On August 3, 2022, the Government of India withdrew the Indian Data Protection Bill (the "Bill") that was pending before the Indian Parliament. The Bill was expected to be tabled during the Monsoon session of Parliament, which commenced on July 18, 2022. While the Government was contemplating making certain changes to the existing Bill, it is now considering drafting fresh legislation, including a bill that addresses a broader range of issues in the digital ecosystem beyond data protection alone of institute.

Day to day we find human rights violations and privacy of an individual is at stake with the recent advancement in the cyber space. The incident of Chandigarh University MMS occurred in September, 2022 is not an exception.

Cyber space is an intangible dimension that is impossible to govern and regulate using conventional law. Cybercrimes have no jurisdictional boundaries.

WHICH RIGHTS ARE HUMAN RIGHTS?

There is difference between human rights in general paradigm and cyber paradigm. For example, everyone is having right to freedom of expression, this right shall include freedom to seek, receive and impart information and ideas of all kinds.

The United Nations Human Rights Commission (UNHRC) has stated that the freedom of expression and information under Article 19 of the ICCPR (International Covenant on Civil and Political Rights) includes the freedom to receive and communicate information, ideas and opinions through the internet.

ARTICLE 19 READS AS UNDER;

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (order public), or of public health or morals.

Laws seeking to balance rights and responsibilities often distinguish between public and private conduct. It is commonly understood that human rights dealt with certain traditional areas such as custodial violence, project displacement, right over resources, sexual harassment, child abuse, tribes etc. A prioritising of rights that has occurred particularly through the agency of the court, and even at the human rights and development communities have been working at breaking down the barriers between rights.

The internationalising of human tights has had a range of effects. International pressure, both from governments and from organisations such as Amnesty International, led to the government establishing the NHRC. The link that is made between human rights and trade, and the 'social clause' that has been under discussion, has, on the other hand, resulted in a wariness – both with the state, and among a number of human rights and development activist.

Liberalisation and globalisation have, again, reoriented government position with regard to the right to work. An emerging enquiry into an element of reinterpreting of rights which occurs in the process of globalisation.

Section 2 (d) of Protection of Human Rights Act, 1993 (amended Act, 2019) defines 'human rights mean the rights relating to life, liberty, equality and dignity of the individual guaranteed by the Constitution or embodied in the International Covenants and enforceable by courts in India.'

The term 'human rights' itself denotes rights relating to the aspects enunciated in the definition. Hence it would be rights of humans relating to their life, liberty, equality and dignity as against the rights with regard to their properties.

Such human rights relating to life, liberty, dignity and equality, effectively come into play when the act of State by virtue of any legislation or delegated legislation is considered: to cite it was considered by the Hon'ble Supreme Court of India in the case of Shantistar Builders v. Narayan Khimalal Totame (1990) 1 SCC 520.

Human rights are rights that belong to every person, and do not depend on the specifics of the individual or the relationship between the right holder and the right grantor.

VIOLATION OF HUMAN RIGHTS

In the digital age misuse of information and technology can take place in relation to any sector; government or private sector activities too. In addition, human rights abuses can arise from the actions of individuals, which give rise to the need for governments to enact laws to protect citizens. technologies are relevant to infringements of human rights include; the internet, techniques, biometric identification, CCTV, mobile phone cameras, listening devices, network database, etc. Many of these technologies were developed by the military and security industry in the 1940s during the Cold War for policing and national security purposes. Since the 1990s, their miniaturization and power has increased immensely. It needs to be emphasised that potential infringements of human rights most often arise following the introduction of legislative measures designed to regulate these new technologies, rather than from the creation or usage of the technologies themselves.

Nature of Human Rights	**Possible areas of human rights violations**
Human freedom and dignity	Electronic surveillance (listening devices, CCTV) Data Machines
Freedom from discrimination	Cyber Racism Computer addiction
Freedom of thought and expression	Online content Surveillance devices Cyber bullying Cyber sexism
Right to bodily security and freedom from inhuman punishments	Electronic tagging Embedded computer chips Biometric identification Death Sentences
Right to a fair trial, presumption of innocence, freedom from self-incrimination	Use of electronic evidence in court Co-mingling electronic evidence Access to online information
Right to own property and protect intellectual property	Digital piracy Computer hacking Electronic espionage
Right to privacy	Electronic surveillance Data machines e-commerce marketing and spam
Right to life	Cyber terrorism

PREVENTION OF VIOLATION OF HUMAN RIGHTS

Ultimately, the prevention of human rights infringements in the digital age lies with individual legislatures which should ensure that new legislation complies with current international and local normative instruments. In addition, the private sector could play a part in preventing abuses by designing new technologies in ways that prevent or minimize potential human rights abuses. Thus, the protection of human rights can best be achieved through an interaction between technological innovation and policy reform. First, hardware and software developers could be persuaded to build into new products technological solutions to problems that concern human rights when developing new technologies. An example is the use of systems which prevent illegal copying of data to protect copyright.

Second, it is important for the human rights implications of new technologies to be examined before they are introduced, and the desirability of establishing global principles to guide the use of new technologies.

Finally, rigorous evaluative research needs to be conducted once new technologies have been introduced in order to monitor their potential for denigration of human rights and infringements of international and national laws. The reporting requirements under international law should be taken seriously by governments and individuals and organizations should be encouraged to report infringing practices immediately they appear.

Human interaction today has significantly changed with the pervasiveness of new communication technology. Social media has proven to be a truly powerful storytelling tool, especially for human rights activists working globally. Human rights education and advocacy thrives on connection; civil society connecting with each other and activists in dialogue with the government on a platform that is widely accessible.

In quashing Section 66A, in Shreya Singhal vs. Union of India (AIR 2015 SC 1523), the Supreme Court has not only given a fresh lease of life to free speech in India, but has also performed its role as a constitutional court for Indians. The Court has provided the jurisprudence of free speech with an enhanced and rare clarity. This judgment provided a much-needed remedy to curb the arbitrary and unjustified powers under section 66A, which amounted to blatant violation of the basic human right of an individual to express his opinion. Through this case, the Apex court has redefined the boundaries of freedoms enjoyed by an individual.

Cybercrime violates human rights such as right to privacy, right to secrecy, right to free from any kind of blackmailing and torture. Hackers usually lock secret data of the user or of any company and demand ransom to unlock them, they also steal data and misuse them. Like in the recent case they hacked twitter account of many well-known persons and misuses their account to collect money by fraud, some demanded money to give back their account. They blackmail and violates children rights by using their videos and picture on different sites.

Nasscom v Ajay shood and others (119 (2005) DLT 596, 2005 (30) PTC 437 Del) - It was a landmark judgment by the Delhi High Court, phishing' on the internet was declared to be an illegal act, entailing an injunction and recovery of damages. Court stated that phishing is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc.

The Delhi HC stated that even though there is no specific legislation in India to penalize phishing still the court held the act of phishing as passing off and tarnishing the Nasscom's image.

In the case of Faheema Shirin RK v. State of Kerala and others, AIR 2020 Ker 35, the Kerala High Court held that Right of Access of Internet is a fundamental right which is guaranteed to all the citizens of the Country. In the year 2017, Kerala became the first state of India which has declared that access to Internet is a basic human right. As a result, the government of Kerala has provided free internet connections to the persons belonging to poor families and at marginalised rate to the others. Though this the government would provide easy access to both governmental and non-governmental services in Kerala.

In the case of Yahoo v. Akash Arora (1999) DLT 285, the defendant made created a similar page as Yahoo and used the same to cheat and influence people. Phishing attack having high intensity is called as whaling attack. In this cyberattack the offender will steal the identity of the victim and will use this identity to make purchase in the name of the victim. The concept of Identity theft scams existed even before the advent of Internet, but with the help of Internet it has been easy for the offenders to obtain information and identity of the victim within no time. In order to prevent such identity theft scams, regular update of various accounts of should be done.

In the case of Gagan Harsh Sharma v. State of Maharashtra (2019 Cri. L. J. 1398) the accused persons were guilty of identity theft of their employer and thus were convicted under IT Act and IPC.

The people using social media are prone to the risk of human rights violations. The unique user ID which is provided by the social media is easily accessible to the other users of the social media. Such easy accessibility, often leads to invasion of human right of privacy of the individuals, which is not only a human right but also a fundamental right as was held in the case of Justice K.S. Puttaswamy v. Union of India, 2017 10 SCC 1.

The Information Technology Act contains special provisions for the purpose of dealing with cyber-crimes. The act punishes such persons who damages the computer system of the other person without the permission of the owner. When a person tries to hack or steal passwords and digital signature of another person then the act punishes the offender with the offence of causing identity theft. The act also punishes child pornography as a cybercrime. The act also punishes possession and distribution of obscene materials which was held in the case of Sharat Babu Digumarti v. Government of NCT of Delhi, (AIR 2017 SC 150).

LITERATURE REVIEW

The intersection of human rights and cybercrime has been a topic of increasing significance due to the proliferation of digital technology. This section reviews key scholarly contributions to the discourse surrounding cybercrime and its impact on fundamental human rights.

THEORETICAL PERSPECTIVES ON HUMAN RIGHTS AND CYBERSPACE

Scholars such as Usha Ramanathan (2001) argue that the digital world has created new domains where traditional human rights laws struggle to maintain relevance. Arup and Tucker (1998) further elaborate on how information technology law has reshaped legal norms, emphasizing the necessity for a global governance framework to address emerging threats.

CYBERSECURITY POLICIES AND HUMAN RIGHTS PROTECTION

The National Cyber Security Policy (2013), formulated by the Government of India, provides a foundational framework to mitigate cyber threats. However, several researchers critique its effectiveness in addressing privacy rights and data protection. The withdrawal of the Personal Data Protection Bill (2022) has further exacerbated concerns regarding the absence of a strong data governance structure in India.

JUDICIAL PRECEDENTS ON CYBERCRIME AND HUMAN RIGHTS

Landmark cases such as Shreya Singhal v. Union of India (2015) and Justice K.S. Puttaswamy v. Union of India (2017) have significantly influenced the legal landscape of digital rights in India. These cases underscore the importance of protecting freedom of expression and privacy from arbitrary state actions.

EMERGING THREATS: CYBERBULLYING, SURVEILLANCE, AND DIGITAL FRAUD

Numerous studies highlight the prevalence of cyberbullying and its psychological impact on individuals. Amnesty International’s research on digital rights violations suggests that online harassment disproportionately affects marginalized communities, reinforcing systemic discrimination.

COMPARATIVE ANALYSIS OF GLOBAL CYBERCRIME LEGISLATION

International frameworks such as the General Data Protection Regulation (GDPR) of the European Union serve as exemplary models for data privacy protection. Studies comparing Indian cyber laws with GDPR emphasize the need for stronger regulatory mechanisms in India.

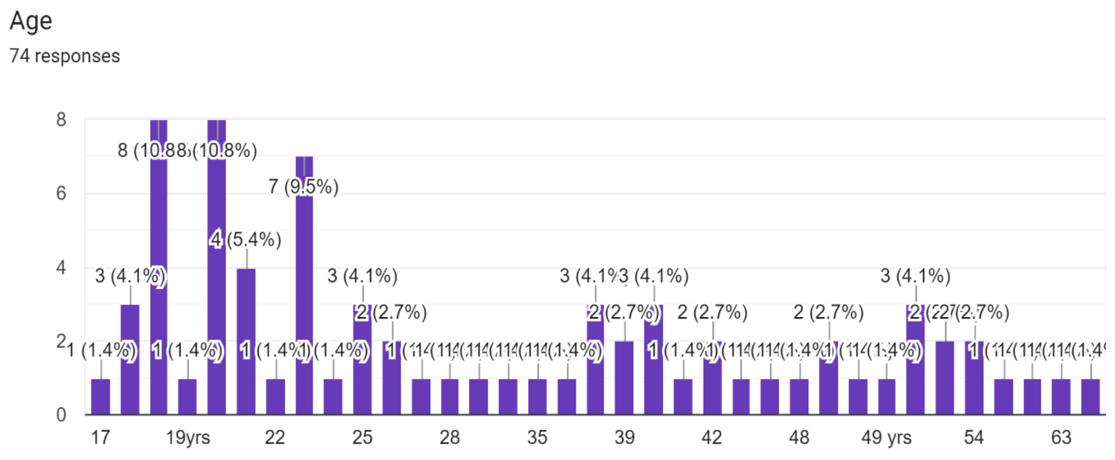
DATA ANALYSIS

Researchers has collected data from the available and willing 74 individuals from different age group about their perception and experience towards the involvement of violation of human rights in cyber-crime. The analysis of the same is as follows.

Personal profile – This analysis firstly probes into knowing the age and gender of the subject. These two factors help in collectively understanding and determining the social attitudes, experiences, and awareness of different age groups and genders toward the issue of cybercrimes.

AGE

In the present study, an attempt has been made to find out the age distribution of the individuals.

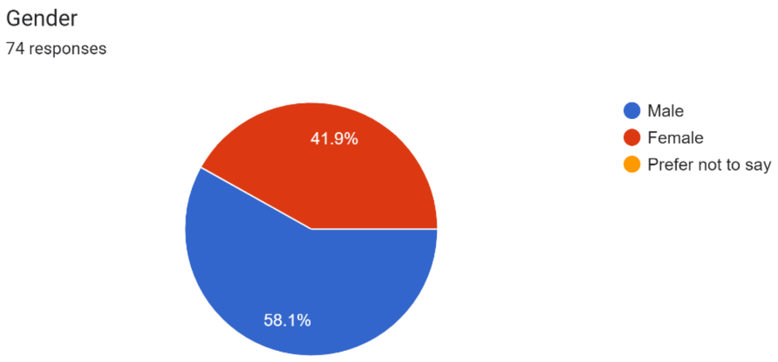


To simplify the above data let us look at the following table.

AGE	FREQUENCY	PERCENTAGE
17-35	43	58.10%
35-50	19	25.67%
Above 50	12	16.21%

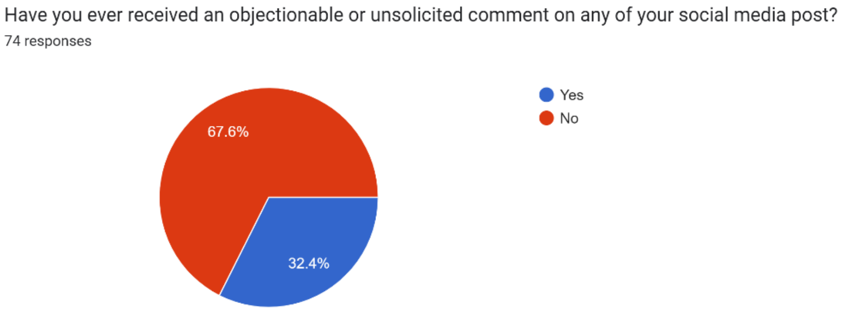
- It is found that majority of the individuals who participated in contributing their responses belong to the age group between 17-35. This group majorly comprises the student and newly employed people. This age group becomes quite relevant as it suggests more involvement of these individuals in the usage of electronic devices and social networking sites.
- Whereas it is seen that individuals belonging to the age groups 35 – 50 are relatively more than those belonging to the age group of above 50.
- This sample even suggests that exposure of middle-aged and old-aged individuals to electronic devices and social networking sites is relatively lesser.

GENDER



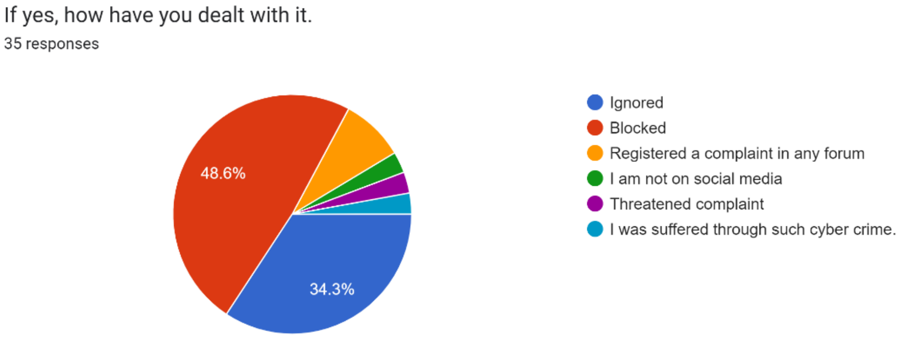
The gender distribution of the individuals who participated in contributing their responses is approximately a ratio of 6:4 between the male and females.

HAVE YOU EVER RECEIVED AN OBJECTIONABLE OR UNSOLICITED COMMENT ON ANY OF YOUR SOCIAL MEDIA POST? IF YES, HOW HAVE YOU DEALT WITH IT.



Have you ever received an objectionable or unsolicited comment on any of your social media post?

74 responses



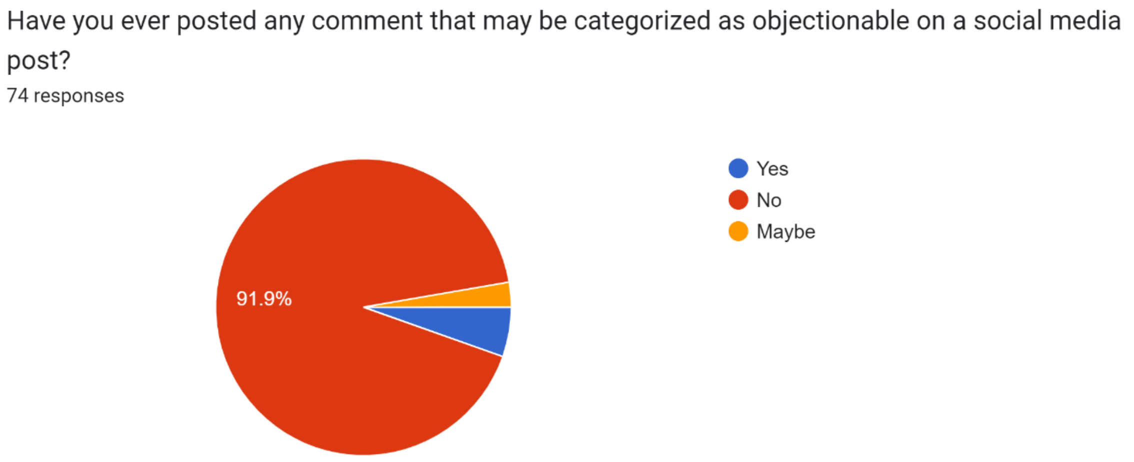
If yes, how have you dealt with it.

35 responses

- It is irrefutable that social media has become an inevitable part of an individual's life currently. The purpose for which an individual may use it varies from educational purposes to entertainment. Nevertheless, at one point or another other, quite a few individuals become a victim of objectionable or unsolicited comments.
- Through this survey, it has been revealed that around 67% of individuals have not fallen prey to such unsolicited remarks. However, there exists around 32.4% of individuals whose privacy has been breached by an objectionable or unsolicited comment through their social media posts.
- However, it is even more surprising to see; how differently each person who faced such comments dealt with such a situation.
- A sizeable 48.6% of the people chose to block such a user. The remaining 34.3% simply ignored this instance and went on with their lives.
- Only 8.6% of the users chose to register a complaint.

- This helps us to conclude that in most situations people take affirmative action against the perpetrator by either blocking or secondly registering a complaint against them. However, still, a staggering 34.3% ignored this occurrence which shows that they are unaware of the redressal techniques or find engaging in such redressal techniques as futile.

HAVE YOU EVER POSTED ANY COMMENT THAT MAY BE CATEGORIZED AS OBJECTIONABLE ON A SOCIAL MEDIA POST? IF YES, WHY SO?

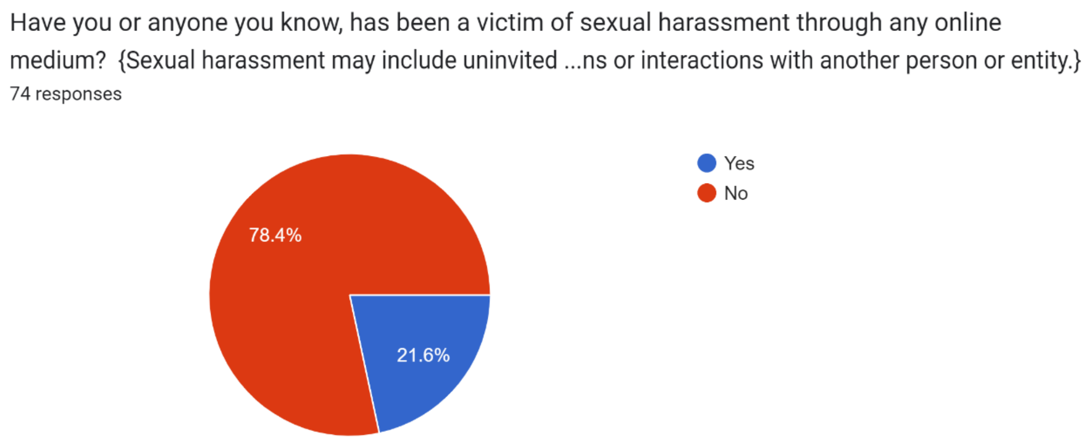


Have you ever posted any comment that may be categorized as objectionable on a social media post?

74 responses

- When the survey inquired about an individual themselves posting an objectionable post a significant number i.e. 91.9% of the people responded as no.
- But a certain 8.1% of the individuals said that they have or might have. And out of these most of them claim that they simply did it for fun or as sarcasm.
- However, it is also to be understood that these people who post something objectionable merely out of fun do not understand the consequences and effect their actions would have on the other person.

HAVE YOU OR ANYONE YOU KNOW, HAS BEEN A VICTIM OF SEXUAL HARASSMENT THROUGH ANY ONLINE MEDIUM? IF YES, KINDLY ELABORATE. {SEXUAL HARASSMENT MAY INCLUDE UNINVITED ADVANCES, COMMUNICATIONS OR INTERACTIONS WITH ANOTHER PERSON OR ENTITY.}

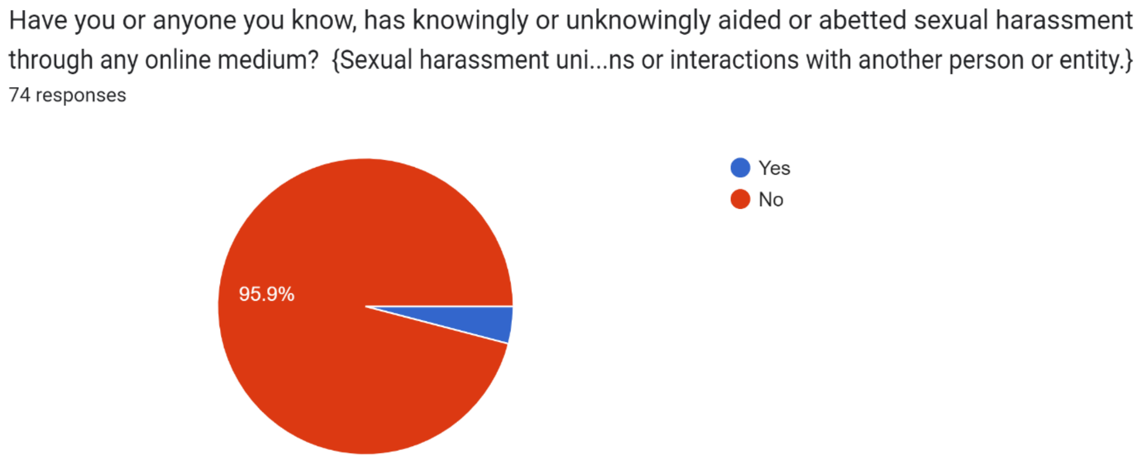


Have you or anyone you know, has been a victim of sexual harassment through any online medium? {Sexual harassment may include uninvited ...ns or interactions with another person or entity.}

74 responses

- When people were asked about being victimized sexually as one form of cybercrime; 78.4% responded of not having experienced or have known of anyone experiencing it. But around 21.6% of people said they have had instances of such an experience.
- Of these, 21.6% were those of second-hand experience wherein certain social media personalities, their friends, or acquaintances experienced unsolicited sexual advances, obscene and vulgar messages along with instances of blackmailing.

HAVE YOU OR ANYONE YOU KNOW, KNOWINGLY OR UNKNOWINGLY AIDED OR ABETTED SEXUAL HARASSMENT THROUGH ANY ONLINE MEDIUM? IF YES, KINDLY ELABORATE. {SEXUAL HARASSMENT IS UNINVITED ADVANCES, COMMUNICATIONS, OR INTERACTIONS WITH ANOTHER PERSON OR ENTITY.}

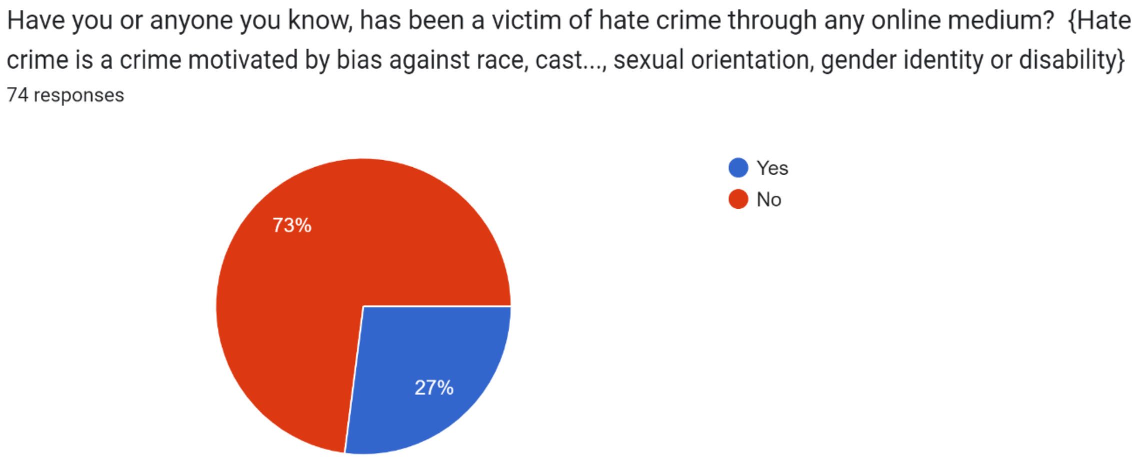


Have you or anyone you know, has knowingly or unknowingly aided or abetted sexual harassment through any online medium? {Sexual harassment uni...ns or interactions with another person or entity.}

74 responses

When individuals were asked about aiding or abetting sexual harassment a staggering 95.9% of the participants in the survey responded no. However, the remaining 4.1% who answered chose to answer this question as yes gave a reasoning that the perpetrator's identity is not revealed most of the time due to the armour of anonymity that web provides.

HAVE YOU OR ANYONE YOU KNOW, BEEN A VICTIM OF HATE CRIME THROUGH ANY ONLINE MEDIUM? IF YES, KINDLY ELABORATE. {HATE CRIME IS A CRIME MOTIVATED BY BIAS AGAINST RACE, CASTE, RELIGION, NATIONAL ORIGIN, SEXUAL ORIENTATION, GENDER IDENTITY, OR DISABILITY}

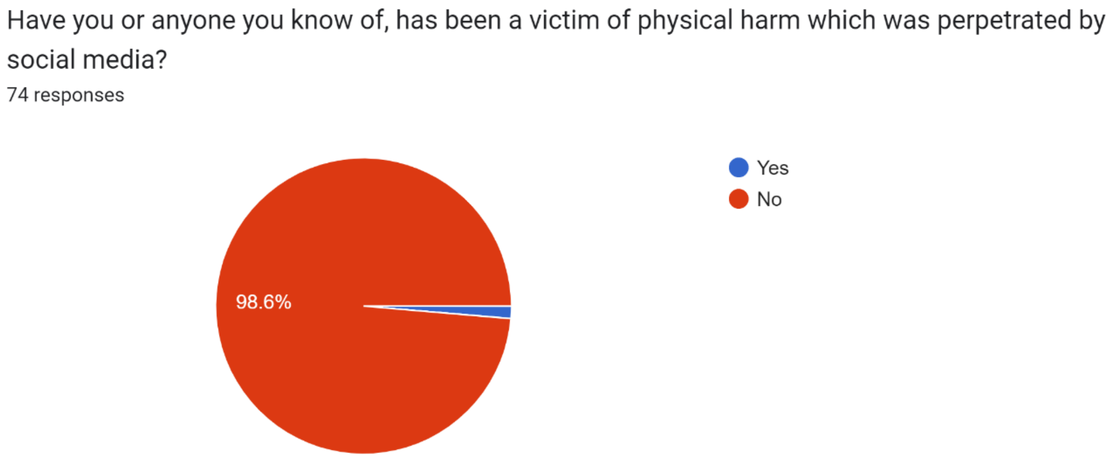


Have you or anyone you know, has been a victim of hate crime through any online medium? {Hate crime is a crime motivated by bias against race, cast..., sexual orientation, gender identity or disability}

74 responses

- With regards to hate crimes 73% of people claimed to not have first or second-handedly experienced it.
- However, 27% of people claimed to have known happening of such things through an online medium. Most of these hate comments usually take the form and shape of instances of body shaming, through offensive memes, because of colour and race, caste, or religion.
- It can also be seen that most of these hate comments come out of a place of communal hatred. While putting down their experiences most of them highlighted the unfair messages being bombarded on minor communities, especially the Muslims.

HAVE YOU OR ANYONE YOU KNOW OF, HAS BEEN A VICTIM OF PHYSICAL HARM WHICH WAS PERPETRATED BY SOCIAL MEDIA? IF YES, KINDLY ELABORATE.

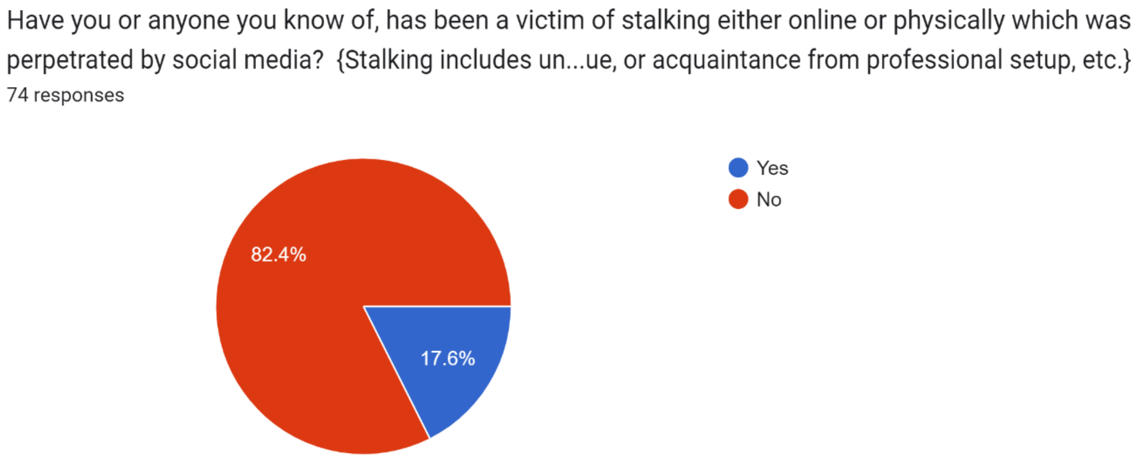


Have you or anyone you know of, has been a victim of physical harm which was perpetrated by social media?

74 responses

- A considerable number i.e. 98.6% of the people responded no when they were asked if they or anybody they knew had been a victim of physical harm perpetrated by social media. But a minor number of 1.4% said that they did.
- And the explanation offered by them reflected such harm usually stems from socio-political violence.

HAVE YOU OR ANYONE YOU KNOW OF, HAS BEEN A VICTIM OF STALKING EITHER ONLINE OR PHYSICALLY WHICH WAS PERPETRATED BY SOCIAL MEDIA? {STALKING INCLUDES UNWANTED SURVEILLANCE BY A RANDOM INDIVIDUAL, COLLEAGUE, OR ACQUAINTANCE FROM A PROFESSIONAL SETUP, ETC.} IF YES, KINDLY ELABORATE.

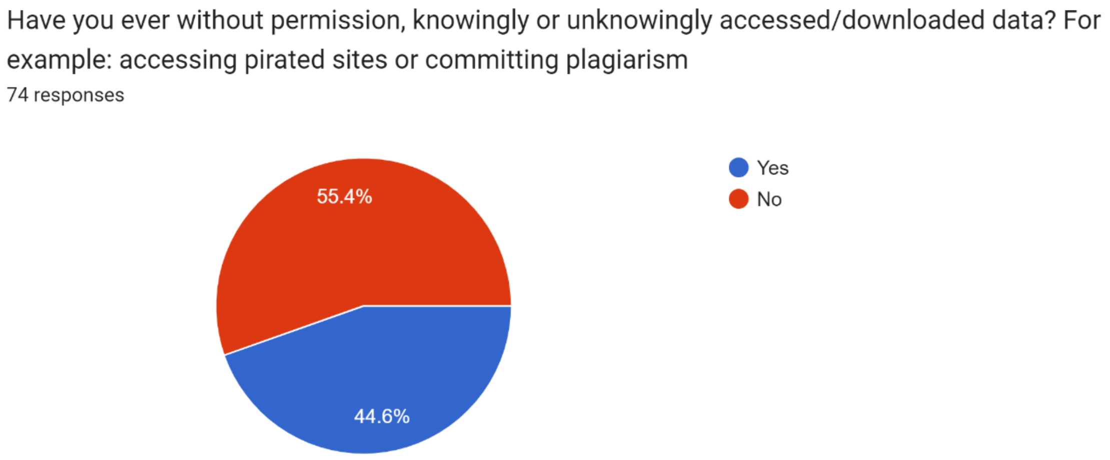


Have you or anyone you know of, has been a victim of stalking either online or physically which was perpetrated by social media? {Stalking includes un...ue, or acquaintance from professional setup, etc.}

74 responses

- The survey reflects that around 82.4% have not experienced or are known to have experienced instances of stalking.
- However, 17.6% of the participants who answered yes gave a detailed elaboration of such instances.
- In most of these instances, Instagram was the common platform through which an anonymous person created fake profiles and persistently tried to follow and get in touch with the victim. And when they were denied access through online mediums it takes the form of physical stalking.
- Apart from anonymous stalkers sometimes acquaintances like a husband stalked his wife. This happened in a Domestic Violence case wherein the husband wanted to keep track of his wife's activities and even tried to humiliate her on social media platforms.

HAVE YOU EVER WITHOUT PERMISSION, KNOWINGLY OR UNKNOWINGLY ACCESSED/DOWNLOADED DATA? FOR EXAMPLE: ACCESSING PIRATED SITES OR COMMITTING PLAGIARISM.

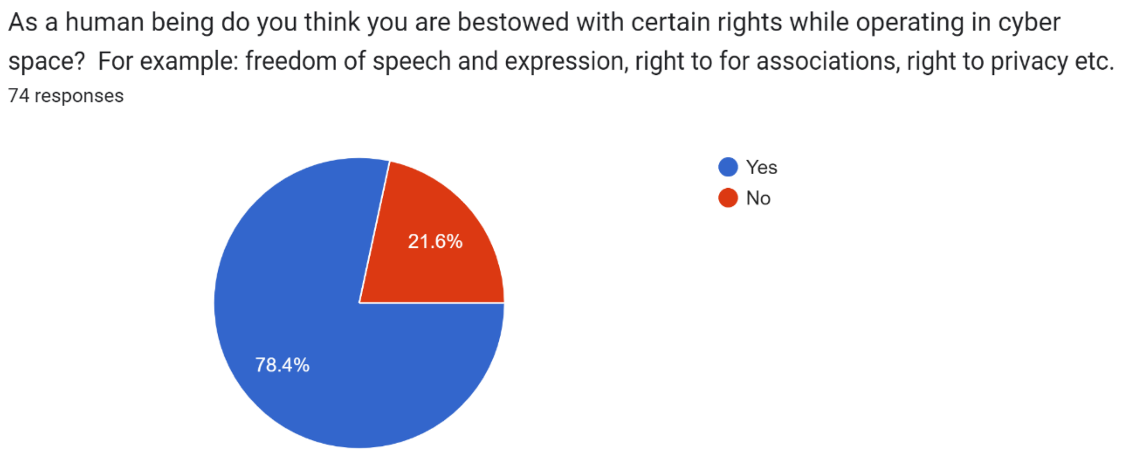


Have you ever without permission, knowingly or unknowingly accessed/downloaded data? For example: accessing pirated sites or committing plagiarism

74 responses

- Through the survey, it can be concluded that almost 44.6% admitted to having accessed pirated sites or having committed plagiarism.
- It can be seen that compared to other breaches and forms of cybercrime this one is much more prevalent.
- Most people are not even aware that this activity actually accounts for a violation of privacy and the stealing of data.
- It is due to this unawareness that the frequency of this crime is more.

AS A HUMAN BEING DO YOU THINK YOU ARE BESTOWED WITH CERTAIN RIGHTS WHILE OPERATING IN CYBERSPACE? FOR EXAMPLE, FREEDOM OF SPEECH AND EXPRESSION, RIGHT TO FORM ASSOCIATIONS, RIGHT TO PRIVACY, ETC.

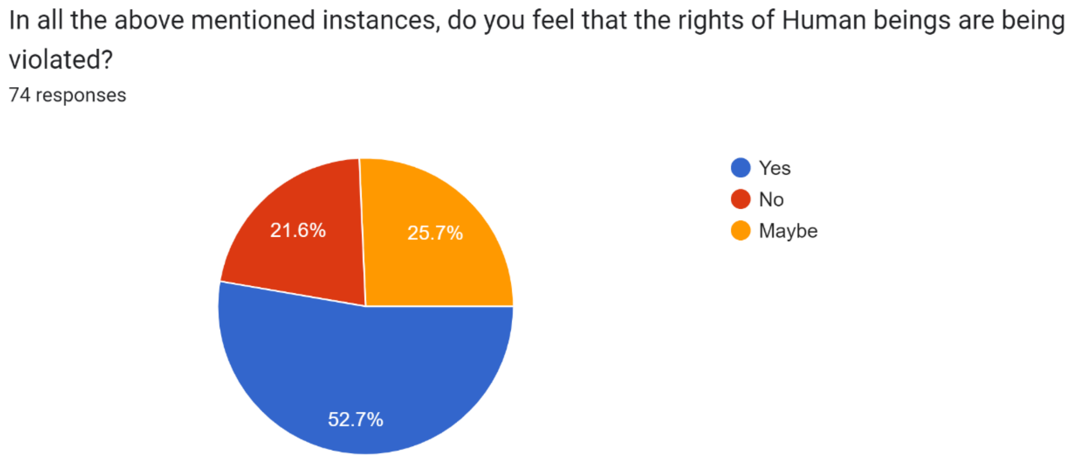


As a human being do you think you are bestowed with certain rights while operating in cyber space? For example: freedom of speech and expression, right to for associations, right to privacy etc.

74 responses

This survey collectively helps in concluding that almost 78.4% of the people who participated in the survey agreed to the fact that humans have integral rights such as freedom of speech and expression and privacy even while operating in cyberspace. Nevertheless, 21.6% of them claim that human beings do not have or have to surrender these rights while operating in cyberspace.

IN ALL THE ABOVE-MENTIONED INSTANCES, DO YOU FEEL THAT THE RIGHTS OF HUMAN BEINGS ARE BEING VIOLATED?

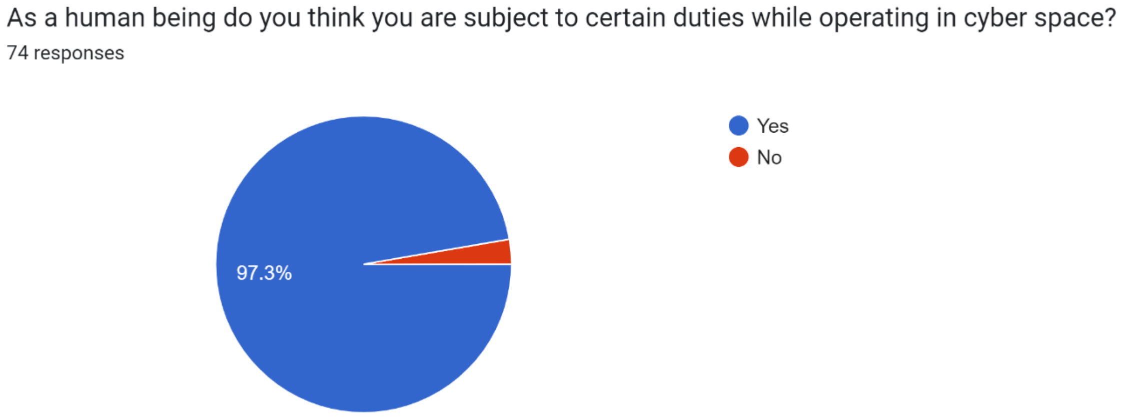


In all the above mentioned instances, do you feel that the rights of Human beings are being violated?

74 responses

- Almost half of the individuals who participated in the survey feel that instances of unsolicited comments, sexual harassment, stalking, hate crimes, etc, in cyberspace violate the integral rights bestowed upon humans.
- However, ¼ of the people who participated are unsure of whether such instances even amount to a breach of rights. The rest 21.6% of the people have firmly taken a stand by responding as no.
- People who admitted that Humans rights are breached generally believe in the fact every individual has a right to own private and personal space.
- They also believe that any act that is impermissible in offline mode should also be impermissible in online mode. And that this should be propagated through awareness.

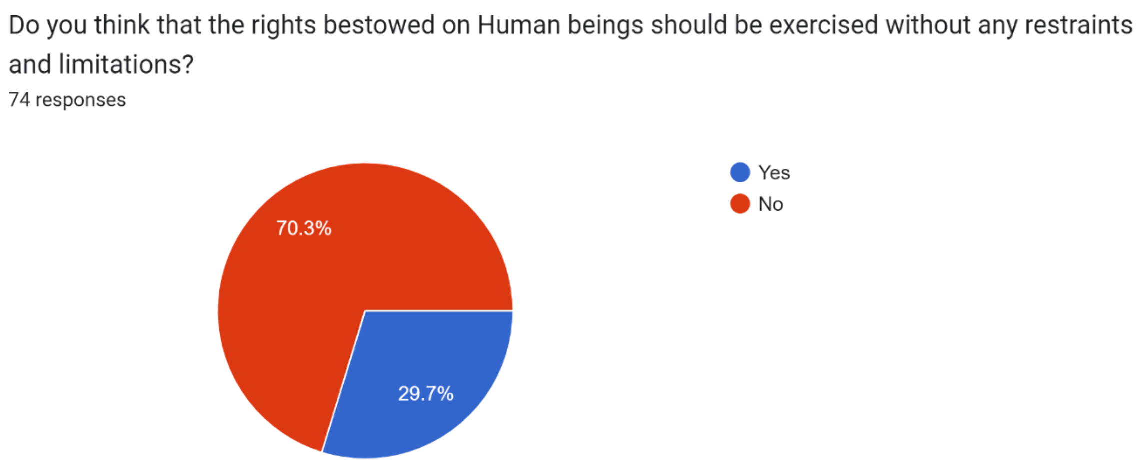
AS A HUMAN BEING DO YOU THINK YOU ARE SUBJECT TO CERTAIN DUTIES WHILE OPERATING IN CYBERSPACE?


As a human being do you think you are subject to certain duties while operating in cyber space?

74 responses

- It is surprising to see that when individuals were asked about whether Human beings have rights in cyberspace only a 78.4% replied in affirmative.
- However, when they were asked if they think individuals have duties while operating in cyberspace a staggering amount of 97.3% of people responded yes.
- Thus, the trend of people giving more weightage to duties rather than enforcement of rights is quite evident.

DO YOU THINK THAT THE RIGHTS BESTOWED ON HUMAN BEINGS SHOULD BE EXERCISED WITHOUT ANY RESTRAINTS AND LIMITATIONS?

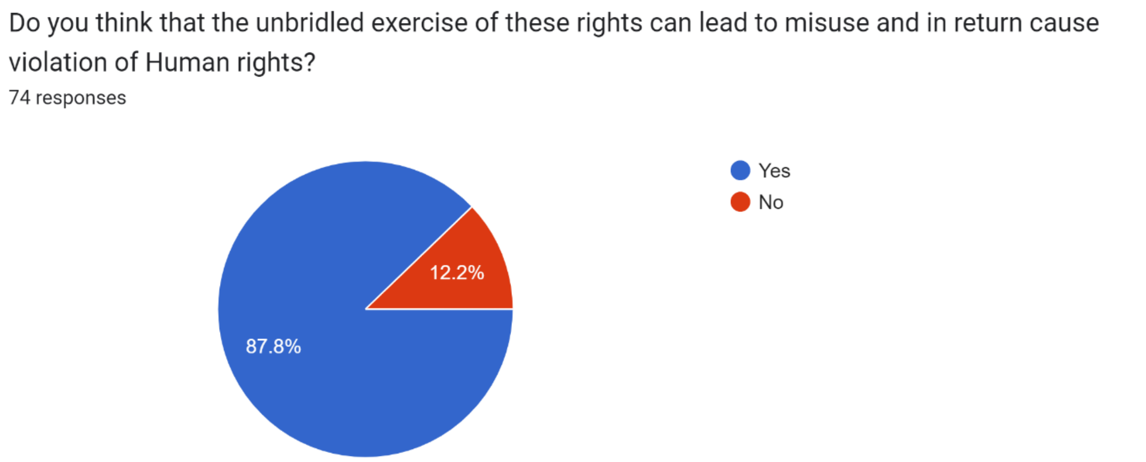


Do you think that the rights bestowed on Human beings should be exercised without any restraints and limitations?

74 responses

It is crucial to understand the trend between the last three questions which delved into the ratio of people believing in the presence of rights and those owing duties while operating in cyberspace. To go further on, it can be concluded that almost 70.3% of the people who participated in the survey believed that though there are rights bestowed upon humans they are subject to restrictions and limitations. And should be exercised discreetly.

DO YOU THINK THAT THE UNBRIDLED EXERCISE OF THESE RIGHTS CAN LEAD TO MISUSE AND IN RETURN CAUSE VIOLATION OF HUMAN RIGHTS?



Do you think that the unbridled exercise of these rights can lead to misuse and in return cause violation of Human rights?

74 responses

- When individuals were asked about the need to limit the exercise of their rights their answer was a strong affirmative. As 87.8% of people believe that the unbridled exercise of rights can lead to misuse leading to violation of human rights.

IF YES, PLEASE ELABORATE UPON THE NEED FOR BALANCE BETWEEN THE RIGHTS AND DUTIES OF HUMAN BEING WHILE OPERATING IN CYBERSPACE.

- The individuals who participated in the survey elaborated the following:
- They expressed the need to have a balance between rights and duties as everyone is obliged to respect everyone and each opinion.
- People should be responsible and not take advantage of anonymity while operating in cyberspace just like a person doing certain things in public.
- Most of them have agreed that the unbridled exercise of rights can lead to chaos without any scope for controlling any mishap. Although while focusing on the need to have reasonable restrictions they have expressed the need to have unambiguous laws and strict boundaries.

KINDLY GIVE YOUR SUGGESTIONS AS TO WHAT SHOULD BE DONE BY THE LEGISLATORS AND POLICYMAKERS TO MAKE CYBERSPACE SAFE AND LESS INTRUSIVE.

• The existing legislation on cybercrimes is considered adequate, but the focus should now be on their implementation. A major issue faced by individuals is the lack of efficient customer care helplines dedicated to each platform, with slow or no responses. Legislators should consider this while formulating and implementing cybercrime policies.

• Key points to address include personal security to prevent account hacking, restrictions on abusive language, and the need for comprehensive standards and outcomes rather than a single policy or solution. Public awareness about rights and responsibilities in cyberspace, emergency protocols for cyber crimes, and privacy protection are essential.

• Suggestions include enacting legislation to restrict the misuse of cyberspace, establishing surveillance programs to identify offenders, imposing stricter punitive measures, and creating tribunals dedicated to cybercrime cases. Education and awareness about cybercrimes should be increased to prevent people from falling victim to predatory content, especially among teenagers.

- Users should be aware of accessing official websites instead of proxy ones, and authorities should take reports on social media seriously. Data protection measures are crucial, and awareness about safe cyber practices should be prioritized. Collaboration with stakeholders such as law enforcement and social media companies is recommended for effective solutions.

- Additional recommendations involve verifying the account holder's identity on social media platforms, banning objectionable words and content, strict action against hate speech, and requiring validation of subscriber addresses for mobile numbers. It is essential for laws to deter cyber harassment and respect freedom of speech and expression.

- Overall, safe cyberspace requires a combination of powerful legislation, strict implementation, surveillance mechanisms, identity verification, penalties for wrongdoers, awareness campaigns, and improved investigation training for law enforcement officials.

ACCORDING TO YOU, WHAT DUTIES SHOULD BE FOLLOWED BY NETIZENS TO MAKE CYBERSPACE SAFER AND LESS INTRUSIVE?

- The law requires individuals to exercise their emotions and prudence while using social media. Trolling and abusive language should be avoided, and responsible behavior is encouraged. Measures like implementing multi-factor authentication and updating software should be taken to enhance security.

- Knowledge sharing and reporting of crimes can contribute to learning from mistakes. Cyberspace should be used for good purposes and not to create chaos or violate someone's rights. Verifying followers and speaking out against cybercrimes are important.

- Awareness of official websites and responsible behavior on social platforms is necessary. Personal information should not be shared, and identity verification is crucial. Cyber privacy should be protected, and cyber security should be maintained. Respect for others, avoiding unnecessary comments, and breaking the chain of negative actions are advised.

- Government-issued SIM cards and tracking of cybercriminals are suggested. Respecting privacy, being cautious with links, and avoiding spreading rumors are important. Following guidelines, being open to different cultures and opinions, and respecting others' rights are emphasized.

- Personal data should not be compromised, and objectionable posts should be ignored. Netizens should be mindful of their impact on society and exercise self-restraint. Respect, privacy, and responsible online communication are key. Illegal activities should be avoided, and knowledge should be improved.

- Social responsibility and securing accounts are important. Annoying content and harmful actions should be avoided. Threats, lies, and personal details should not be shared. The safety of others and responsible usage of social media should be prioritized. Freedom of expression should be respected within legal boundaries. Awareness, responsibility, and protection of others' rights are essential.

- Precautions should be shared to prevent cyber crimes. Stalking, hate speech, and personal information should be avoided. Netizens should use cyberspace for personal growth, exercise self-control, and contribute positively to the community. Safe search and awareness of fraud are recommended.

CONCLUSION

The purpose of the present discussion is not to assess whether legislation in India relevant to cybercrime compiles with complies with each Convention or piece of legislation, but rather to indicate some areas in which human rights concerns have been identified, and also to point to potential areas of infringement, if certain technological developments occur. At present India can be guided by what has occurred in various overseas countries which have enacted local human rights legislation, or whose legislation has been challenged in the Human Rights Commission or higher courts.

While the unfettered existence of cybercrimes highlights the lack of truth, accountability and remedy in relation to the human rights violations. Social media has proven to be a truly powerful storytelling tool, especially for human rights activists working globally. From a political standpoint, Cyber Platforms have provided human rights advocates with an opportunity to advance civil liberties especially in countries where freedom of speech is significantly curtailed. The internet has allowed individuals to freely express and disseminate their opinions to a large global audience.

However, the Internet also provides a new and powerful medium through which persons can publish hateful or discriminatory comments, and intimidate and harass others, in a manner which undermines the human rights of those who are targeted. Accordingly, societies' use of the Internet raises challenging questions about the appropriate balancing of rights in cyberspace. Difficult questions of how to simultaneously protect potentially competing rights are not unique to the online environment. But the particular features of the Internet its global and therefore cross-jurisdictional and instant reach; its creation of an effectively permanent record of communications, and the ability to communicate anonymously present new obstacles for governments seeking to protect against harmful behaviour.

There are two broad challenges regarding human rights and use of the Internet which emerge from the discussion in this paper, namely:

1. How do we as a society achieve an appropriate balance between competing rights in an online environment?

2. What steps should be taken to address violation of human rights in terms of the ability of certain groups to access and safely utilise the Internet?

Addressing violation of human rights in terms of access to and use of the internet in the growing importance of the internet to all aspects of life; including delivery of services by business and government; means that the 'digital divide' between those with effective access to the internet and those without limits the latter group's ability to enjoy a range of human rights.

In order to effectively address this gap in enjoyment of rights (particularly the right to freedom of expression and information), consideration should be given to the following:

(a) What groups are affected by the 'digital divide'?

(b) To what extent does this impact on their enjoyment of rights?

(c) What measures should be taken to address the difficulties that the following groups may experience in accessing the Internet:

(i) people with disability

(ii) Senior Citizens

(iii) Indigenous people

(iv) Indians living in remote or rural areas?

To what extent would the 'digital divide' be addressed by ensuring access for all citizens to internet facilities? How relevant are issues such as digital literacy and cyber-crime to the effective enjoyment of rights through the Internet for these groups?

Balancing rights online a key challenge in terms of ensuring that individual's rights are protected online; is achieving by an appropriate balance between protecting the right to freedom of opinion and expression in cyberspace, and protecting people from online bullying, discrimination and harassment which breaches their rights.

The types of issues which need to be explored include:

(a) How prevalent is online hate speech (i. e. racial vilification, hate speech against women, LGBTI people) - is it only a small minority who posts this extreme content, or is there a wider problem?

(b) Are online hate speech, discrimination and verbal abuse different to hate speech, discrimination and verbal abuse that occur in the offline world - does the potential reach and permanency of internet content change the impacts of these types of behaviours?

(c) Are legislative measures, rendering behaviour unlawful or criminal, an appropriate and/or effective way of achieving a balance between the competing rights in an online environment?

(d) For the purposes of the application of effective laws, what should be considered a 'public' vs. a 'private' space in the online world?

(e) To what extent are preventative educative measures an effective way of addressing violation of human rights?

(f) What type of laws, polices and/or practices do we need to create safe online environments for children, to ensure that they enjoy their rights in cyberspace; including the right to freedom of expression and to information?

The widespread penetration of cyberspace has both empowered and threatened human rights. The evolution of cybercrimes, including identity theft, digital fraud, cyberstalking, and hate speech, highlights the urgent need for an effective legal and regulatory framework

KEY FINDINGS FROM THE RESEARCH INDICATE

1. Need for Robust Cyber Laws – India's existing legal framework, including the IT Act, lacks comprehensiveness in addressing new-age cyber threats.
2. Digital Literacy and Awareness – Many users remain unaware of their digital rights and responsibilities, leading to increased cybercrime vulnerability.
3. Privacy and Data Protection – The absence of stringent data protection laws increases risks associated with unauthorized data usage and breaches.
4. Government and Private Sector Collaboration – Addressing cyber threats requires multi-stakeholder participation, including tech companies, law enforcement, and policymakers.

RECOMMENDATIONS FOR FUTURE POLICY MEASURES:

- Implementation of a comprehensive Data Protection Law in India.

- Strengthening judicial mechanisms for redressal of cyber rights violations.
- Mandatory cybersecurity awareness programs to educate individuals on digital rights.
- International collaboration for cross-border cybercrime prevention.

By addressing these concerns, policymakers can create a balanced and secure cyberspace where technological advancements serve humanity rather than violate fundamental rights.

REFERENCES

1. https://www.meity.gov.in/content/national-cyber-security-policy-2013-1 (14.09.2022)
2. https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 (14.09.2022)
3. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (14.09.2022)
4. https://humanrights.gov.au/our-work/rights-and-freedoms/publications/background-paper-human-rights-cyberspace (14.09.2022)
5. Usha Ramanathan, Human Rights in India A Mapping, https://www.ielrc.org/content/w0103.pdf (14.09.2022)
6. Arup, C., & Tucker, G. (1998). Information technology law and human rights. In Kinley, D (ed) Human Rights in Australian Law. (pp 243-66), Federation Press: Sydney.
7. Faheema Shirin RK v. State of Kerala and others, AIR 2020 Ker 35
8. A.G. Noorani, Cyberspace and Citizen's Rights, 32 Econ. Political Wkly. 1299,1299 (1997) https://www.jstor.org/stable/4405474.
9. Yahoo v. Akash Arora, 78 (1999) DLT 285
10. Gagan Harsh Sharma v. State of Maharashtra, 2019 CriLJ 1398
11. Justice K.S. Puttaswamy v. Union of India, 2017 10 SCC 1.
12. Sharat Babu Digumarti v. Government of NCT of Delhi, AIR 2017 SC 150.