# HOW DO SOCIAL MEDIA AND AI BRING TOWARDS THE DOOMSDAY OF THE INTERNET?

**Shashank Sharma[*] Amritansh Bansal[*]**

## INTRODUCTION

The Internet is a vast global network that facilitates people to communicate, connect, and exchange data with each other; it also helps us access various resources, from websites to social media, online services, and more. The Internet helps us connect with millions of private and public networks worldwide. The internet is also known as "**ARPANET**" It was one of the US government research that came in the 1960s to 1970s. Over time, it was fully developed and has been made public in the late 1980s and early 1990s.

After the advent of the internet in the early 1980s, there has been tremendous development in the field of information technology. Now, 70% of the global GDP is managed because of the Internet.

The internet allows us to communicate with each other through various things, and it works on different protocols, such as-

1. TCP/IP
2. HTTP/HTTPS
3. DNS

Now, the internet works through different browsers such as Google Chrome, Firefox, Brave, Safari, etc. Through these, we can access various servers to access the website and use or collect the data from it. With the advancement of the internet, there were few sources made to connect and communicate easily everywhere this is where social media came into the picture. It has a tremendous effect on society; social media makes everything easy for people in the form of communication and sources of information.

The internet has transformed everything around society, and it also has effects on Communication, Education, Business, Entertainment and other aspects of society. It has made

[*]BBA LLB, THIRD YEAR, FAIRFIELD INSTITUTE OF MANAGEMENT AND TECHNOLOGY, NEW DELHI.
[*]BBA LLB, FOURTH YEAR, MANAV RACHNA INTERNATIONAL UNIVERSITY, FARIDABAD.

life so easy that all the information can be accessed within a few seconds. It also connects people across the globe, but with such advancement, there are also security reasons and privacy breaches.

Now, after the development of the internet, humans, with its help, have created two new technologies called Artificial Intelligence (AI) and social media, in today's world, AI is used for preparing summaries and researching large amounts of data, also there are plenty of AI tools which help students in their assignments and homework, whereas social is used for creating photos, videos, sharing ideas and communicating with other people.

One of the things that we see changing swiftly in this era is the shift of traditional sources of knowledge, that is, books, to new and advent sources such as AI. AI is also generally used in a lawyer's office for preparing drafts for legal documentation and effectively analysing the factual matrix of the cases. With the advent of optical fibres and high-speed data networks, human civilisation has risen from the ancient Indus Valley to the one reaching the moon.

## INTRODUCTION TO AI AND SOCIAL MEDIA

AI and Social media are some of the rapidly growing technologies in the world. These two technologies change the era of books and older-generation messaging platforms.

AI can be defined as a computer-controlled individual that does things that a normal human being can do and comprehend. AI can work and adapt to the experience or the details that are fed to it. AI was introduced in 1956, but this term was only used in sci-fi movies or scientific research until the working AI comes into the real world like "Chatgpt". Ai is also said to be known for decision-making based on logic and rules.

AI is not only of one type it is divided based on their working, and few of them are said to be theoretical. These AI are:-

1. **Artificial narrow** intelligence is called weak AI it is the only AI that is there, and any other AI is theoretical. This type of AI can be used to get a single task or simple task done, and at a faster rate than a human being, it cannot do any task beyond the given command.
2. **General AI**:-Artificial general intelligence(AGI) is also called as strong AI this type of AI is only said to be theoretical because in this type it can learn, store and use the previous skills to get the work done by any human command or without the training of the human being.

3. **Super AI** is commonly said to be super artificial intelligence this AI is also said to be theoretical as it is said to be the same as AGI, but in this, its function would be having the human emotions and have the mind of their own.

Social media is one of the platforms in which multiple resources are provided; it can be understood as the platform from which a person can communicate and share ideas and information, not only that, but it also allows the user to create photos and videos and share them with other people. Through social media, an individual can not only interact with people within the region but also globally, and it helps them build their connections. It also has a feature for creating groups; it helps not to message a person individually, but instead, you can send or share the information with a large number of people.

With so many opportunities and making life easier for people, it leads to the misuse of the services that are provided by social media as it allows the user to share photos or videos of their family or post something personal on social media sometimes, it can lead to the security risks like hacking, phishing, online harassment, Stalking etc.

## HOW DOES AI AND SOCIAL MEDIA AFFECT THE INTERNET?

We talk about the ascendency of AI, the Internet, and Social Media, considering how it changed the workplace, the marketing strategy, the way of communicating with people, etc. We must not forget that there are several hidden swindles related to it, which indeed affects not only society at large but even most of the minds of the younger generations since they have constant access to the internet at their fingertips. The most common things that are happening nowadays are cyberbullying, hacking, stalking, and the ill use of AI tools. AI has gone from the best possible way to do work to the use of creating fake images and videos to threaten people, blackmail them, and then use it in the worst possible manner.

With the advent of the internet and, thereafter, social media. The merger of the latter two changed our world and our perspective on it. Though it only came with the idea of making lives leisurely for the people since every coin has two sides, so social media, because of which nowadays people have started making negative remarks about other people, with an intent to defame them publicly on the platform to gain a handful of likes and comment. Those comments, which people may not remember the very next minute. Because of this considerable factor, it made the lives of people, especially the content creators, miserable and also affected their mental health as well. There is also a wave on the very social media platforms where

people are spreading misinformation and lies about each other to gain fame and publicity on such platforms. Given the rapid advancement and proliferation of Artificial Intelligence, it is crucial to recognise the extensive range of potential illicit applications that accompany these technological developments. The remarkable progress in AI brings with it not only transformative opportunities but also significant ethical and security challenges. The emergence of sophisticated AI systems necessitates a thorough assessment of the potential misuse of such technologies. It is indeed essential to understand that these considerations must be meticulously addressed to pre-emptively identify and mitigate the risks associated with the malicious deployment and use of AI tools. Thus, before the implementation and reliance on AI technologies, a rigorous evaluation of their possible adverse applications and associated ethical implications is imperative. Ensuring that such evaluations are integral to the deployment strategy will help safeguard against unintended consequences and uphold the integrity of AI usage.

Talking about AI and data protection, we must not forget the latter Puttaswamy Judgement, which was **Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[1].** In the Puttaswamy Judgement, the Hon'ble Supreme Court of India recognised the Right to Privacy as a Fundamental Right, guaranteed under Article 21 of the Constitution of India, 1950. The ruling of the Supreme Court specifically mentions the fact that in today's digital world, we need to protect the personal data and information of people from various programs and applications based on Artificial Intelligence.



## HOW DOES THE INTERNET AFFECT THE HUMAN MIND

### Cyberbullying

In today's world of Social Media, where every person, irrespective of / age ranging from young children to old people, has personal social media accounts, people also tend to upload their memories and other relevant videos and photographs and also use several social media platforms to interact with people miles away, this leads to the notorious problem of identity deception by various people to young children, who therefore tend to act as a young mind to their age but behind the screen, it is a masked person who deceives himself to be a young mind and has the intention to deceive children by various means and then later extracting ransom

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017): SC. Via Indian Kanoon. https://indiankanoon.org/doc/127517806/ Accessed on 4th September, 2024

from them by blackmailing them. This is one of the most common problems faced by many young children nowadays.

And most of the common things that happen nowadays are Cyberbullying. It is defined as aggressive behaviour that is done by an individual or a group of people on social media platforms repeatedly against a victim over some time, who, being a victim, cannot easily defend himself or herself alone. It is said to be done in the form of hate comments, body shaming, racism, etc. There are different types of cyberbullying commonly known to us, out of which some of them are-

1. Cyberstalking
2. Doxxing
3. Impersonation

These are the forms of cyberbullying that come under Cyberbullying. Though seemingly similar. But these have different meanings. It is said to be done by different methods, too. Talking in depth about the latter, we come to know that-

1. **Cyberstalking:** Cyberstalking is a practice of using electronic modes of communication such as emails, text messages or audio messages for which the sender of these messages has an illicit intention to stalk/harass a person or a group. It is said to be more perilous than other forms of cyberbullying as it is adjacent to the threat to people's safety online.

Cyberstalking may also include Monitoring a person constantly, Identity Thefts, Threats, Vandalism, Solicitation for sex, or gathering information that may be used to threaten or harass the victim.

**Landmark Judgement on Cyber Stalking-**

Little did Seema Khanna[2] (name changed), an employee with an embassy in New Delhi, know that web surfing would lead to an invasion of her privacy. In an apparent case of cyberstalking, Khanna received a series of emails from a man asking her to either pose in the nude for him or

[2] Rohit Lohia, 'Cyber Stalking in India' (2019), Legal Service India < https://www.legalserviceindia.com/legal/article-1048-cyber-stalking-in-india.html > 7th September, 2024

pay Rs 1 lakh to him. In her complaint to Delhi Police, the woman said she started receiving these emails in the third week of November.

The accused threatened Khanna that he would put her morphed pictures on display on sex websites, along with her telephone number and address. He also allegedly threatened to put up these pictures in her neighbourhood in southwest Delhi.

Initially, she ignored the emails, but soon she started receiving letters through post, repeating the same threat. She was forced to report the matter to the police, said an officer with the cybercrime cell.

That, however, was not the end of her ordeal. The accused mailed the woman her photographs. The woman claimed these were the same photographs that she had kept in her mail folder. The police said the accused had hacked her e-mail password, which enabled him to access the pictures.

A preliminary inquiry into the complaint has revealed that the emails were sent to the victim from a cyber cafe in south Delhi. We hope to trace the accused soon, said Deputy Commissioner of Police (crime) Deependra Pathak.

The police feel the accused might be known to the victim as he seemed to know a lot about her. The cyberstalker can be booked under Section 509 of the IPC for outraging the modesty of a woman and also under the Information Technology Act, 2000. (From 1st July 2024, section 509 of The Indian Penal Code falls under Section 79 of Bharitya Nyaya Sanhita, 2024.)



**2. Doxxing:** Though Doxxing has not been expressly defined in any code about the jurisdictional scope of India, in the eves of law, generally, It is the act of revealing somebody's personal information that is known to you online, that too without his or her consent and which should have caused the other person, whose identity has been revealed, severe damages.

**Complaint on Doxxing-**

Several comedians, such as Vir Das, Rohan Joshi and Kaneez Surka, have alleged in the public domain that their personal contact information and addresses were leaked, which subjected them to threats and abusive messages by the general public.

One day, a Twitter user shared screenshots of jokes from some comics - including Varun Grover, Aditi Mittal, and Abish Matthew - which they had cracked in the past. The social media users claimed the comedians particularly used Hindu gods in their joke punchlines and started trending.

One day, the private contact details of these comedians were shared from an anonymous Twitter account. The account was later suspended. Joshi, co-founder and member of the now-defunct comedy group AIB, took to Instagram and requested that his family be spared of the abuses coming his way. He also offered an apology for hurting any religious sentiments. Vir Das said that many comedians, including himself, were at the receiving end of such hate messages.

Another comedian named Radhika Vaz said she, too, was getting trolled. She wrote on the microblogging site, too.

The development came days after a female stand-up comic was subjected to online rape threats and abuses after a year-old video of her allegedly cracking a joke on Chhatrapati Shivaji Maharaj's statue surfaced.

The National Commission for Women (NCW) on Sunday sought immediate action from Gujarat Police against one Shubham Mishra for allegedly hurling abuses and giving rape threats to the said comedian on social media.



Vadodara Police had arrested Mishra on Sunday for the alleged video. Mumbai Police's Cyber Branch, too, took Suo Moto cognisance of another alleged threatening video against the comedian and arrested Imtiyaz Sheikh, who used the profile 'Umesh Dada' on YouTube, on Monday.

Reacting to the threats against the female stand-up comic, comedian Sumukhi Suresh on Sunday wrote being hurt over a joke is not an excuse to give "rape threats" to artists.

This case is related to the abuse and harassment of standup comedians by the general public. This cannot be categorised as Doxxing, but the judge in the said case connected this to the

concept of Doxxing as it included the Personal Information of the comedians, i.e. their phone numbers and addresses were leaked and circulated online. [3]

**3. Impersonation:** Impersonation in Indian Laws is defined as "The act of pretending to be someone else, which you are not or knowingly substituting one person for another person by their deceiving identity."

**Essential of impersonation-**

1. **Assuming of false identity:** Talking about the concept of Assumption of a false identity under Indian law, it can be clearly understood that it is an offence under Bharatiya Nyaya Sanhita (BNS), 2024, where "A person is said to Cheat by personation, where he cheats by pretending to be someone else, or by knowingly substituting one person for another to deceive people, or by representing that the other person is a person, other than the person who he is". One of the famous Judgments we study under this concept is mentioned below-

**Sucha Singh Mann vs State of Punjab on 8 December 2022[4]**: This is one of the famous cases of the Hon'ble Supreme Court of India, related to the concept of assumption of false identity. The case talks about how Four petitions were filed about a single FIR involving allegations of forgery and fraud. The FIR was lodged by Resham Singh Maan against Mohammad Saheed and his wife, Sulekha Khatun, alleging they had forged documents and used them to open a bank account. The key allegations were that Saheed impersonated Resham Singh's brother to claim a share in family land. The police investigation recommended charges under various sections of the Indian Penal Code (IPC). Sucha Singh Mann, another brother, was also implicated in the case. He filed a revision petition, challenging the framing of charges against him. The revision court modified the charges, leading to further petitions by Sucha Singh and Resham Singh. The petitions raised various grounds, including lack of evidence, delay in filing the FIR, violation of procedural rights, and malicious prosecution. The parties presented arguments and relied on legal precedents to support their positions. The final resolution of the petitions will depend on the court's assessment of the evidence, the merits of the arguments, and the applicable legal principles.

[3] Complaint against Standup comedian Vir Das for allegedly using derogatory statements against India during his concert in the U.S.
[3] Sucha Singh Mann V. The State of Punjab (2022): SC. Via Indian Kanoon. https://www.casemine.com/judgement/in/56ea8137607dba378d9d30e1 Accessed on 8th September, 2024

**2. Pretending to hold a public servant:** If anyone in India falsely represents himself/herself to hold the post of any public servant, which he/she is not entitled to do so, and such act is done to fraud the society, in other words the act of committing deceitful or dishonest action to gain advantage or benefit, then he/she would be said to have committed the offence of "Personating a public servant" under "Section 204 of The Bhartiya Nyaya Sanhita." One of the relevant cases, which we study under the topic is-

**State of Punjab & Ors V. Prem Swaroop (2008) SC[5]:** In this case, the respondent Prem Swaroop was a police constable who was accused of impersonating a government official and was convicted. However, on appeal, he was acquitted due to insufficient shreds of evidence against him. Despite this, a disciplinary proceeding was initiated against him, resulting in a punishment of forfeiture of his salary. The respondent challenged the disciplinary action, arguing that his acquittal should preclude any departmental punishment. The High Court dismissed the respondent's appeal, finding that the evidence in the criminal case was not considered by the disciplinary authority. The Supreme Court of India later considered the matter, examining whether the respondent's acquittal should have protected him from departmental punishment under the relevant police rules. And held that the respondent shall be presumed guilty under section 170 of The Indian Penal Code, 1860 and shall be tried according to the provisions of the law. (As of 1st July 2024, the Indian Penal Code has been repealed, and the section of "Personating a public servant" has now been covered under section 204 of Bhartiya Nyaya Sanhita, 2024.)



3. **Falsely representing a person or organisation:** In the context of India, falsely representing a person or an organisation by using their credentials and business data that are available publicly on the internet can cause a lot of serious damage to the company or any organisation or a person which can even lead to reputation damage, heavy financial losses, civil liabilities along with criminal charges. They also affected the company's goodwill in the market as they used their name to fraud other people, which led to the downfall of the company. Under "Section 447" of The Companies Act 2013[6], there has been an express mentioned about the "Punishment for Fraud", which explains, "If any person commits any fraud, involving an amount of at least ten lakhs rupees or 1% of the total turnover of the company, the latter shall be punished an imprisonment, minimum of 6 months to 10 years, and shall also be liable to

[5] State of Punjab and Ors. V. Prem Swaroop (2008): SC. Via Indian Kanoon. https://indiankanoon.org/doc/1024425/ Accessed on 6th September, 2024
[6] Section 447 of The Companies Act, 2013

fine, which shall not be less than the amount involved in the fraud". In India, other than the provisions of the Companies Act 2013, there have been several legal provisions which have been created to safeguard other companies from these types of cases. This has been clearly explained under "Section 319"[7] of the Bhartiya Nyaya Sanhita (BNS), which deals with the offence of Cheating and Impersonation. Another section of the law that is relevant and can be held applicable is section 336[8] of Bhartiya Nyaya Sanhita, which deals with the offence of Forgery. One of the landmark judgements of India, which we study in the context of impersonation, is-

**Aloke Nath Dutta & Ors V State Of West Bengal (2006):** [9]The case of Alok Nath Dutta deals with the issue of where a small building was owned by Arunamoyee Dutta, whose son Aloke Nath was residing there. Due to the property disputes, Aloke confessed that he impersonated Biswanth, his brother, along with various accomplices, to sell the property and later murdered him. The Hon'ble Supreme Court of India, on 12th December 2006, found Alok to be guilty of Impersonation and Murder of his brother Biswanth, due to which he was awarded a Death Penalty by the Hon'ble Supreme Court of India. It was in this case that the Supreme Court of India considered the doctrine of "Rarest of the Rare", which was established in the case of Bacchan Singh V. State of Punjab in 1980.

Considering the latter Aloke Nath Judgement by the Hon'ble Supreme Court of India, we now must also throw some light onto the types of Impersonation which hold utmost relevance while discussing the concept of Impersonation.

**Types of Impersonation**

**Criminal Impersonation:** Criminal Impersonation, as per law, can be defined as a practice where someone intentionally pretends to be someone else to deceive, defraud and harm others. Through this, the impersonator gains several advantages, such as extracting money, property, or other advantages. The abovementioned judgment of the Hon'ble Supreme Court of India in the matter of Aloke Nath Dutta & Ors V. The State of West Bengal can be held relevant in the context of Criminal Impersonation.

[7] Section 319 of BNS, 2024
[8] Section 336 of BNS, 2024
[9] Aloke Nath Dutta & Ors V State Of West Bengal (2006): SC Via Indian Kanoon. https://indiankanoon.org/doc/1522913/ Accessed on 8th September, 2024

**Online Impersonation:** Online impersonation means where one person steals the identity of another person through electronic means, i.e. via the internet, that too, to deceive or harm another person's identity on the internet or any social media platform. One of the landmark judgments of India, which we study in the context of online impersonation, is-

**Rediff Communication Limited v Cyberbooth and Anr[10]:** This case marks one of the landmark judgments by the Hon'ble High Court of Judicature in Bombay, delivered on 15th July 2015. This case revolves around the concept of 'Cybersquatting', wherein the Respondent named Cyberbooth has registered his domain named "Radiff.com". Which was identical to that of the domain of Plaintiff named "Rediff.com"

**Cybercrime**

Cybercrime, in the eyes of the law, in India, is nowhere mentioned officially in any of the Legislation, but in the Internet world, it is defined as an offence that has been committed against any individual or group of individuals to harm their reputation, steal their personal information or cause physical or mental trauma through electronic means. Electronic means can include, but are not limited to, the use of modern telecommunication networks such as the Internet (networks including chat rooms such as Zoom.us and Meet.google.com, emails, E notice boards, and groups) and mobile phones which can be targeted through Bluetooth/SMS).

Whenever a cybercrime happens in any corner of the world, some issues come along with it, studying such issues, we tend to realise that in today's world, cybercrimes, unlike any other crime, are growing several folds which pose a severe threat to the security, personal details and digital identity of the people. This also poses severe threats to the banking details of the people, which ultimately pushes them into heavy financial loss, leaves them with absolutely no money and ultimately pushes them into the loop of the debt trap. Some of the common issues associated with the concept of cybercrime are:

1. **Financial Frauds:** Many cyber attackers tend to keep an eye on and attack the very first moment they get a chance to attack the bank account of individuals or businesses. Ransomware, Phishing, etc, are some of the common examples that ultimately lead to major financial losses to people and business houses at large. Though there have been tremendous advancements in the field of data security and security related to the digitalisation of financial institutions, there

[10] Rediff Communication Limited V. Cyberbooth and Anr (1999): Bombay HC. Via Indian Kanoon. https://indiankanoon.org/doc/806788/ Accessed on 4th September, 2024.

are still a large number of hackers who have become successful in bypassing such security codes. Apart from these, many scams occur through phone calls and SMSs, where people tend to deceive their identity and falsely represent themselves as their Banking Official or Banking Partner and try to extract the banking information such as passwords and usernames from the people with the bait of some freebies and offers. Many people also try to commit various credit card frauds through their phishy online shopping websites. This has ultimately corrupted the market structure, and this also has been categorised as uncompetitive behaviour in the market concerning Competition in India.

**2. Misrepresentation:** A large number of frauds and frivolous organisations are now working on a large scale on a model that revolves around the concept of misrepresentation of the goods/ services they provide to the public. This business model solely works on the principle of misrepresenting goods and services and trying their best to extract as much money as they can from the pocket of the consumer. For instance, A company named PQR will showcase its products through social media and will even mention its official site to buy the product from, but as soon as the consumer logs in to that site with his/her E-mail address, the fellow's email address and passcode will be misused by the website and then several financial or other sorts of frauds can happen with him/her.

**3. Phishing Attacks:** Phishing emails and messages can be used to use the consumers to click on phishy/malicious links websites, which will ultimately lead the consumer into a situation where his/her identity, such as banking details or other personal information. This information can be used to commit identity theft and financial fraud.

4. **Masking of Company**: There are many organisations around the globe, though formed legally, but they still have been doing their dirty work at the back. As of now, they work as call centres and scam people, especially old people, because they seem to be an easy target for them. These organisations have people who don't only work within India but also target people globally as they have employees working for them who can even pretend to be the tech officer of a renowned Tech Giant such as Microsoft, Apple, etc. and get all the personal details including their Social Security Number[11] through which they can access their bank accounts easily. These people mostly use software like "Anydesk" to get access to the systems of the people, and through that, they can get any details of the people that they want.

[11] **Social Security Number:** A nine-digit number issued to permanent residents and citizens to track individuals with social security accounts in the USA.

**Reasons behind the advent of cybercrimes at large:**

**1. Lack of Social Awareness and Education:** In today's world of the internet, many scams are going on, and there is no social awareness and education provided for it, even though it affects society at large. There are many people of different age groups that come under the radar of scammers, and because of the lack of education for cybercrime, they lose a lot of money to these scammers. As a result, many poor or lower-middle-class people are suffering from debts and still have not been able to repay them on time. Many times, scammers can even steal people's money by using their names and user IDs to get access to their personal information without even their notice, which makes people fall victim to cybercrime for which they don't even know the remedies.

**2. Technological Advancements:** Since the advent of the Covid19, the world has shifted from conventional offline platforms to doing work/business and taking things online. "Cloud-based[12] work/jobs" were promoted. Even in the education sector, things went online as many of the Schools/Colleges started delivering lectures to students via online through various platforms such as Zoom.us, Meet.google.com, MS Teams, etc. This global shift due to the pandemic forced people to learn technology and go online, many of the businesses and startups went online to sell their services. This ultimately gave many of the cyber attackers a light to commit more cyber-attacks as a large number of people now have their digital identity on the internet, which they can access now.

**3. Global Internet Usage:** Since the world shifted towards the number of technological advancements, this. As a result, increased global internet usage by several folds, due to which the amount of information people on the internet also increased drastically, this availability of free information gave a bowl full of opportunities to cyber stalkers and hackers, and now they can get every information of the personal life of people and a full details of how they keep and manage their finances. Which makes it easy for "cyber attackers[13]" to commit forgery[14] through the internet.

[12] The delivery of services and products using cloud based software programs, it is also used to provide data storage to people over the internet.
[13] An individual or a group working to access the systems through internet and steal confidential information of the people.
[14] A message where the sender deliberately deceives his identity in order to extract relevant and sensitive information from the receiver.

**4. Lack of proper implementations of IT legislation at ground level:** One of the primary problems that people have to deal with in today's world is the lack of proper implementation of the laws related to Information and Technology, particularly mentioned in the Information and Technology Act, 2000. These cyber laws are made to protect people from various cyber-attacks and also to stop them from falling victim to unethical hacking, phishing, etc., but these Cyber laws are still lacking in several places such as even in today's world number of people are not able to report their cybercrimes to government because of some corrupt and malpractices of the people who work at government places and various cyber cells offices of the state.

Irrespective of such a large number of loopholes, the Government of India has even launched its portal to report Cyber Crime online, known as the National Cyber Crime Report Portal, which works seamlessly without the need for any government official or any corrupt practice in between. This portal serves to redress the grievances of the victims of Cybercrime and serve them with Justice by giving them apt and justified solutions and remedies and also by initiating an investigation against the accused.

## NATIONAL CYBER CRIME REPORT PORTAL

We can report cybercrime on the National Cyber Crime Report Portal, which is an initiative of the government of India to keep track of the existing cybercrimes happening in the country and to take cognisance of such matters as soon as possible.

This portal is an initiative of the Government of India to facilitate victims/complainants to report cybercrime complaints online. It also serves as a user-friendly platform for citizens to report distinct types of cybercrimes securely and anonymously, with a special focus on cybercrimes against women and children. This helps the complainants to keep their identity confidential and

easily report any cybercrime against them. The portal covers offences such as hacking, identity theft, online fraud, and cyberbullying. Users can lodge complaints online, upload relevant evidence, and track the progress of their cases. The portal also offers resources, including cyber safety tips and guidelines to help users prevent cyber incidents. Managed by law enforcement agencies, the National Cyber Crime Reporting Portal aims to safeguard digital infrastructure,

promote cybersecurity awareness, and ensure prompt action against cyber offenders to uphold digital safety across India. Complaints reported on this portal are dealt with by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaints for prompt action.

As a consequence, it recommended that the offence be made gender-neutral. The Justice J.S. Verma Committee, in its report, has also defined stalking in a gender-neutral language. Therefore, it has been proposed that stalking be made a non-bailable as well as a gender-neutral offence. Justice J.S. Verma was a renowned Indian jurist who eventually served as the Judge of the Hon'ble Supreme Court of India and later served as the 27th CJI.

## CONCLUSION

To sum up everything that has been stated so far, we have now concluded that the internet, being a worldwide network of networks, facilitates communication, information sharing, education, etc., on a large scale. In today's world, many of the everyday tasks are done through AI, which is used to prepare summaries, drafts, etc, which are particularly used in the lawyer's office. Nowadays, the Internet is the primary source of information, thus giving birth to Artificial Intelligence, which is a handy tool in the world of the Internet.

AI, establishing its roots in every field, did not leave social media behind. Social Media, being a platform to provide a variety of content productions, is now also taking the help of AI to manage content creation effectively as AI can understand trends and make conclusions from them, thus helping the social media tech giants and content creators to supply the content their audience wants. AI also makes it easier to contact and talk to people living miles away and are of different ethnicity from us due to its algorithm of translating languages instantly. AI and the internet are now two sides of the same coin, but one must not forget the hidden swindles of it. AI and the internet negatively affect young minds as it makes people used to it in no time. With the integration of AI and the internet, there has also been a rise in the issue of privacy and data protection.

Cyberbullying is done by various stalkers on the internet, and their particular targets are children and elderly people enjoying such platforms. Many types of cyberbullying are familiar.

Impersonation is also one of the major problems faced by people, which has two types of it. Online and Criminal. Out of this, the solution and penalisation of Online Impersonation is the need of the hour.

Cybercrime is also on its way to being one of the most committed offences globally, with little or no cures or prevention of it. Many people and cybercrime organisations work on a large scale to commit Financial Fraud against people by misrepresenting themselves. Phishing Attacks are now becoming very common, thus leaving the identity of people at no security. Many people are now running full-fledged companies by falsely representing themselves to be any of the famous and renowned companies of the world and thus deceiving people in their name.

There are several reasons why cybercrimes are increasing at large, such as Lack of Social Awareness and education, Large-scale technological advancements, and the increase in global internet usage. One of the ground reasons for such problems is the improper implementation of IT legislation at the ground level, due to which attackers take advantage of the legislative loopholes and thus, the digital identity of the nation is put at risk.

To establish IT legislation at the grassroots level, there has been an initiative by the Government of India, the National Cyber Crime Report Portal, helping to keep track of cybercrimes happening in India.