INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 14 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ROLE OF A INDIVIDUAL PERSON IN CYBERSPACE REGULATION IN INDIA

AUTHOR - B P SWAROOP ARADHYA, LLM STUDENT, SCHOOL OF LAW, RAMAIAH UNIVERSITY OF APPLIED SCIENCES

BEST CITATION - B P SWAROOP ARADHYA, ROLE OF A INDIVIDUAL PERSON IN CYBERSPACE REGULATION IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (14) OF 2025, PG. 550-557, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI – https://doi.org/10.65393/NDRC4697

ABSTRACT

As technology progressed in India, and as people started adopting technology to their daily life it becomes of utmost important for every person to understand the concepts of cyberspace, cybercrime, Artificial intelligence, cyberspace regulation. By 2030, India's digital economy is projected to contribute nearly one-fifth of the country's overall economy, outpacing the growth of traditional sectors. As we observe the society we notice that there is substantial increase in cyberspace activities as well as increase in cyberspace crime rates. So the regulation of cyberspace is necessary in the form of enacting laws, framing rules and regulations, by which the rights of a individual person is protected. And Individual person also have some responsibility towards cyberspace regulation which cannot be neglected. This article makes a effort to analyse the concept of cyberspace, cybercrime, the rights that are available to a individual person in cyberspace in India and duties of a individual person in cyberspace regulation.

Keywords: *Cyber space, Artificial Intelligence, Cyber Crime, Rights, Duties, Individual person*

I. INTRODUCTION

As technology progressed in society and as more of daily life and business moves online, Cyber crimes have proliferated to large extent. The widespread use of Internet of Things, Artificial intelligence has expanded the opportunities for cyber criminals to commit cyber crimes and exploit people. Cybersecurity incidents in India rose from 10.29 lakh in 2022 to 22.68 lakh in 2024, it indicates the increasing threats and complexity of digital threats in India. At the same time, the financial toll is becoming more pronounced, with cyber frauds amounting to ₹36.45 lakh reported on the National Cyber Crime Reporting Portal (NCRP) as of 28 February 2025. In United states of America The FBI's Internet Crime Complaint Centre reported a 33% increase in losses in 2024 over the previous year, with total losses exceeding $16 billion. From these incidents we can say that cyber crime has to crubbed as soon as possible. And the burden of regulation of cyberspace rests on government as well as on individual. The role of individuals in cyberspace regulation involves individuals becoming a active participants in cyber security and cyber governance. The crucial role of a person is maintaining strong Cyber Hygiene, that is individuals taking responsibility of cyber security by using high security passwords, activation of Multi-Factor Authentication (MFA) on personal accounts, by updating software in personal computers and in mobile phones to patch security vulnerabilities, installing anti-virus software in computers and digital gadgets. And a individual should be a primary defender against cybercrimes by verifying the authenticity of communication before clicking on links or sharing information. Besides these measures a individual should resort in reporting cybercrime activities to regulatory bodies. This paper aims to analyse the role of a individual person in cyberspace regulation .

II. DEFINITION OF CYBERSPACE : Cyberspace is a term which has been interpreted by numerous authors in their own sphere of

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

knowledge. An American Canadian Science fiction author William Gibson in his 'Burning Chrome'(1982) first introduced the term Cyberspace and in his novel Neuromancer (1984) he popularised the term Cyberspace. Ottis, R. & Lorents defines Cyberspace, according to him "cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems." Cyberspace is "the total interconnectedness of human beings through computers and telecommunication without regard to physical geography. Cyberspace transcends geographic and national boundaries The fundamental difference between physical space and cyber space is, **physical space is the tangible, and the real world** we live in, while **cyberspace is a virtual, non-physical realm which is** created by interconnected computer networks.

III. DEFINITION OF ARTIFICIAL INTELLIGENCE Artificial Intelligence can be defined as a technology that would mimic human intelligence. AI is a machine that can simulate human thought process and can take actions based on those thoughts and even draw conclusions. AI refers to the ability of machines to perform cognitive tasks like thinking, perceiving, learning, problem solving and decision making. Jhon McCarthy defines Artificial Intelligence as " the science and engineering of making intelligent machines" And Marvin Minsky defines Artificial Intelligence as "the science of making machines do things that would require intelligence if done by men"

IV. DEFINITION OF CYBER CRIME Cyber Crime can be defined as a criminal activity that occurs through the medium of computers or through internet. Gordon and Ford defined cyber crime as " as any crime involving computers, networks, or hardware". Thomas and Loader defined cyber crime as " computer-mediated acts that are illegal and carried out via global electronic networks". The Oxford Dictionary defines the term cyber crime as "Criminal activities carried out by means of computers or the Internet."

The Russian scholar I. M. Rassolov, in his works, points out the following characteristics of cybercrimes: 1. The use of computer networks and international information exchange, which constitutes the principal distinguishing feature of a crime in the sphere of high technologies. In this case, the computer and its networks act as the object of the crime, the instrument of the crime, or the means on which unlawful acts are prepared.

2. The transnational nature of the crimes under consideration (they are committed in the global information space) and the international character of the participants in the criminal community.

3. A stable tendency toward the "organized" nature of cybercrimes and their expansion beyond national boundaries.

4. The presence of a criminal pyramid consisting of at least three levels of interaction.

There are many types of cybercrimes in cyberspace, some of the types of cybercrimes are Cyber bullying, cyber stalking, cyber grooming, online job fraud, online sextortion, vishing, smishing, simple swap scam, debit card fraud, impersonation and identity theft, phishing, spamming, ransomware, Trojans, data breach, denial of service, website defacement, cybersquatting, pharming, crypto jacking, deepfakes, digital arrest, etc.

V. REASONS FOR THE OCCURRENCE OF CYBERCRIMES AND ARTIFICIAL INTELLIGENCE RELATED CRIMES IN INDIA

The huge boom in the usage of mobile phones by people, and affordable internet data plans for internet access, and usage of online payment systems like UPI for day to day financial transactions, have increased the "attack surface" for criminals. Though the technology as benefited the people by making their life easier than earlier but due to increase in cyberspace activity it has created a larger pool for criminals for targeting victims. As we observe in day to day life our personal computer or computers of a organisation suffer from security vulnerabilities due to poor security systems, use of pirated software, lack of regular

maintenance and software updates creating a environment for cyber criminals to commit cybercrimes. Majority of population in India are unaware of the cybercrimes like phishing links, fake apps, identity theft, social engineering scams, digital arrest, debit card / credit card scams ,etc. Creating a more vulnerable situation to cyber crime to occur. Most cybercrimes are financially driven because of low operational costs and high potential rewards, which is the main reasons for the occurrence of cyber crimes. And the Internet provides a degree of anonymity, which further complicates the identification of criminals. The borderless and transnational nature of cyber crimes also complicates enforcement of law due to different laws and rules prevailing over different countries and the challenges in international cooperation. The main reasons for the occurrence of Artificial Intelligence related crimes is that with even less knowledge about technology, data architecture, programming and coding, cyber criminals can commit cyber crimes using Artificial Intelligence.

VI. HOW CYBERSPACE CAN BE REGULATED

As society progressed and with evolution of digital technology, cyber space regulation becomes of utmost important to protect society from cybercrimes. The question that comes to our mind is how can cyberspace be regulated ?. The answer is cyberspace can be regulated through different mechanisms, among them are through law enforcement, code architecture, social norms, market forces, code of conduct, self regulation of organisations, etc.

Lawrence Lessing in 1998 in his work Laws of cyberspace, and in 1999 Code and Other Laws of cyberspace brings out four forces through which cyber space is regulated, they are Laws, Code architecture, Social norms and Market . According to Lawrence Lessing 'Code is Law' that is code architecture can regulate cyberspace behaviour. So the phrase code is law means that the software and hardware architecture of the internet (the "code") is a powerful regulatory force that effectively governs behaviour in cyberspace, much like traditional government law does in the physical world. But, Cyber Space regulation not only rely on government mechanisms or on code architecture but it also relies on individual persons attitude and behaviour towards cyberspace.

VII. ROLE OF A INDIVIDUAL PERSON IN CYBERSPACE REGULATION IN INDIA

A Individual person play a vital role in cyberspace regulation. Role of a individual person can be viewed in different ways, that is by exercising his rights in cyberspace, performing duties and fulfilling responsibilities towards cyberspace regulation.

A. RIGHTS OF A INDIVIDUAL PERSON IN CYBERSPACE

Rights of a individual person in cyberspace can be inferred as the fundamental right or statutory rights that are guaranteed by Constitution or available to a person by the force of law. The rights of a individual person in cyberspace is of vital importance because by the exercise of these rights in cyberspace a individual also contributes to the regulation of cyberspace.

The Constitution of India guarantees six fundamental rights, under Part III of Indian Constitution that are described in Articles 12 to 35. The freedom of speech and expression is provided under Article 19(1)(a), which extends to all citizens the right to express their views through any medium, including the internet. The right covers cyberspace and the internet also which is a platform for the exercise of free speech. But the right is not absolute it is subject to "reasonable restrictions" under Article 19(2) of the Constitution. Article 19(2) allows the State to impose reasonable restrictions on the right to free speech based on eight grounds that are ; Sovereignty and integrity of India, Security of the State, Friendly relations with foreign States, Public order, Decency or morality, Contempt of Court, Defamation, Incitement to an offense. The Supreme Court of India has affirmed that the internet access and online expression are integral part of the fundamental right. In Shreya Singhal v. Union of India 2015 Supreme Court of

India struck down Section 66A of the Information Technology Act, 2000, relating to restrictions on online speech, as unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the Constitution of India. Court held that Section 66A did not fall under the purview of "reasonable restrictions" permitted by Article 19(2). established that fundamental rights apply fully to the internet and that any legislation seeking to restrict online speech must adhere strictly to the principle of "reasonable restrictions" under Article 19(2). Article 21 of Indian Constitution provides that *No person shall be deprived of his life or personal liberty except according to the procedure established by law."* Article 21 does not explicitly mention right to privacy. In **Justice K.S. Puttaswamy (Retd.) vs Union of India 2017**, **Supreme Court of India** held that the **Right to Privacy is a fundamental right** implicit in **Article 21**. The Court ruled that privacy is essential to human dignity and falls under the ambit of **right to life and personal liberty**.

The Information Technology Act 2000 has a provision under Section 43A for compensation for failure to protect data. The section provides that Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. So the section provides a right for a person to seek compensation for data breaches from a body corporate if it fails in protecting data of a person.

The Information Technology Act 2000 has various sections which lists out cyber crimes and provides for punishment and penalties for those offences, thereby giving the right to persons to seek justice if there rights and liberties are violated or curtailed.

Section 66 says that Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. Section 66 says If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Section 66C says that Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section66D Says that Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E says that Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Section 66F says Whoever,–(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by–(i) denying or cause the denial of access to any person authorised to access computer resource; or (ii) attempting to penetrate or

access a computer resource without authorisation or exceeding authorised access; or (iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or (B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,commits the offence of cyber terrorism. (2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section 67 says that Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A says that Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B says that Whoever,–(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or (d) facilitates abusing children online, or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–(i) the publication of which is proved to be justified as being for the public good on the ground that such book,

pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or(ii) which is kept or used for bona fide heritage or religious purposes. Explanation–For the purposes of this section, ―children‖ means a person who has not completed the age of 18 years.

Section 67C. Says that (1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.(2) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021) provides for diligence by intermediaries and grievance redressal mechanism thereby protecting the rights of a person.

The rights available to a person under The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 are

Right to know the rules, regulations, privacy policies and user agreements of IT intermediaries

Right to have IT intermediary computer resources free from illegal or harmful information

Right to be free from information hosted, displayed etc. by person not having right over and the intermediary shall make reasonable efforts to cause the user of its computer resource not to host, display, information that, belongs to another person and to which the user does not have any right;

Right to be free from information that is obscene, pornographic, paedophilic or invasive of privacy including bodily privacy

Right to be free from information that is insulting or objectionable to a gender, race or ethnicity

Right to be free from information relating to or encouraging money laundering or gambling

Right to be free from information that promotes enmity on grounds of religion or caste

Right to be free from information harmful to child

Right to be free from information that violates intellectual property rights

Right to be free from misinformation and information that is patently false or misleading

Right to be free from information that impersonates another person

Right to be free from information that threatens India's unity, integrity, defence, security or sovereignty, friendly relations with foreign States, or public order, or incites commission of any cognizable offence, or is insulting other nation

Right to be free from information that prevents investigation of any offence

Right to be free from software designed to endanger computer resource

Right to be free from information that violates any Indian law

Right to redress of grievances against IT intermediary

Right to redress of grievances against violation of the IT rules

Right to redress of other grievances against IT intermediary website/app

Right to have information removed from the computer resource of IT intermediary in a time bound manner that is

1. Right to removal, within 24 hours, of content exposing private area of or showing the user of the IT intermediary in the nude or in sexual act, or impersonating or morphing the user's image
2. Right to removal, within 15 days, of information hosted, displayed etc. by person not having any right over it, or violating intellectual property right or any Indian law
3. Right to removal, within 72 hours, of any other information that violates the right to have IT intermediary computer resources free from illegal or harmful information

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 14 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

The Digital Person Data Protection Act 2023 and Digital Person Data Protection Rules 2025 places the individual at the centre of India's data protection system.

The rights available to a person under Digital Person Data Protection Act 2023 and Digital Person Data Protection Rules 2025 are

Right to Give or Refuse Consent Every person has the choice to allow or deny the use of their personal data. Consent must be clear, informed and easy to understand. Individuals may withdraw their consent at any time.

Right to Know How Data is Used Citizens can seek information on what personal data has been collected, why it has been collected and how it is being used. Organisations must provide this information in a simple form.

Right to Access Personal Data Individuals can ask for a copy of their personal data that is held by a Data Fiduciary.

Right to Correct Personal Data People may request corrections to personal data that is inaccurate or incomplete.

Right to Update Personal Data Citizens can ask for changes when their details have altered, such as a new address or updated contact number.

Right to Erase Personal Data Individuals may request the removal of personal data in certain situations. The Data Fiduciary must consider and act on this request within the permitted time.

Right to Nominate Another Person Every individual can appoint someone to exercise their data rights on their behalf. This is helpful in cases of illness or other limitations.

Mandatory Response within Ninety Days Data Fiduciaries are required to address all requests related to access, correction, updating or erasure within a maximum of ninety days, ensuring timely action and accountability.

Protection During Personal Data Breaches If a breach takes place, citizens must be informed at the earliest. The message must explain what happened and what steps they can take. This helps people act quickly to reduce harm.

Clear Contact for Queries and Complaints Data Fiduciaries must provide a point of contact for questions relating to personal data. This may be a designated officer or a Data Protection Officer.

B. DUTIES AND RESPONSIBILITIES OF A INDIVIDUAL PERSON IN CYBERSPACE

Rights and duties are two sides of a same coin. Duties can be defined as obligations or responsibilities that an individual is expected to perform. We can infer that duties of a person is important as much as right of a person. In cyberspace every individual has a duty to act according to Law of the land, and to behave responsibly and ethically. In cyberspace a individual person has some duties and responsibilities so that the person rights are protected and the rights of other person are not violated.

The duties and responsibilities are

To safeguard personal information by strong password

To regularly update software and devices in order to prevent cyber vulnerabilities

To use firewall and antivirus tools to protect system

To report suspicious activities to authorities

To respect privacy of others in cyberspace

To maintain decorum in cyberspace

To cooperate with law enforcement in cybercrime investigation

To avoid sharing sensitive data over digital media

To be aware of the rights that are available to a person in cyberspace

Besides these, The Digital Person Data Protection Act 2023, in Section 15 provides for some duties that a data principal shall perform, that is

(a) comply with the provisions of all applicable laws for the time being in force

while exercising rights under the provisions of this Act;

(b) to ensure not to impersonate another person while providing her personal

data for a specified purpose;

(c) to ensure not to suppress any material information while providing her

personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;

(d) to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board; and

(e) to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure under the provisions of this Act or the rules made thereunder.

VII. CONCLUSION

Cyberspace is a evolving concept, due to its dynamic nature sometimes it becomes difficult to understand its nature. As of now the world is progressing towards technological advancement including progress in the field of artificial intelligence, as we get closer towards technology our life are getting better at the same time we are facing difficulties in regulation of cyberspace as our rights are getting violated in the form of cybercrimes. So it important for a state to protect the rights of a individual person, and protect the state from cybercrimes. But cyberspace regulation means not only enforcing rights of a individual person but individual persons also owe a responsibilities towards the society and state by performing some duties and fulfilling responsibilities. So cyberspace can be regulated with the combined efforts of both state and society. And a individual person plays a pivotal role in cyberspace regulation.

REFERENCE:

[1] https://static.pib.gov.inPDFTen Years of Digital Progress - Building an Inclusive and Future-Ready India
[2] https://www.pib.gov.inCurbing Cyber Frauds in Digital India
[3] www.google.com
[4] https://www.oxfordlearnersdictionaries.comcyb ercrime
[5] https://en.wikipedia.orgCybercrime
[6) https://cybercrime.gov.in/Webform/CrimeCatD es.aspx
[7] https://en.wikipedia.orgCode and Other Laws of Cyberspace
[8] The Constitution of India
[9] https://en.wikipedia.orgShreya Singhal v. Union of India
[10] https://en.wikipedia.orgPuttaswamy v. Union of India
[11] The Information Technology Act 2000
[12] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021)
[13] Digital Person Data Protection Act 2023 and Digital Person Data Protection Rules 2025
[14] https://nludelhi.ac.inPDFA Handbook on Basics of Cyber Hygiene
[15] https://gac.gov.in/CMSData/CMSContent?