

## A STUDY OF RIGHT TO PRIVACY IN DIGITAL SPACE

MANISHA KUMARI<sup>1</sup>

### ABSTRACT:

In digital world, private life of individual has been compromised although legal framework has been developed but frequent cases of breach of privacy by means of computer or computer system and internet are high in number. Unauthorised access to other networks, harassment via e-mail, cracking, hacking, spoofing, page jacking, carding, cyber- stalking and dissemination of obscene materials are crimes which has posed threat to individuals' right to privacy. Cyber space is new place for criminals to commit crime and criminals take advantage of weak framework of cyber laws. Digital space has provided safe heaven to cyber criminals. Cyber security is a matter of grave concern in present digital era. Many times, identity of cyber criminals is not known hence it would not be wrong to say that cyber criminals have privacy in digital space but common public don't have. The present paper will discuss in detail how right to privacy of individual is at stake in digital space and what is legal framework related to cyber space in India.

**Index words: Cyber laws, Internet, Cyber -crime, Cyber security, Right to Privacy.**

---

<sup>1</sup> ASSISTANT PROFESSOR, INDIAN INSTITUTE OF LEGAL STUDIES, AFFILIATED TO UNIVERSITY OF NORTH BENGAL.

## I. INTRODUCTION

Privacy is an inherent aspect of human life. Expansion of utility of technology in every facet of human life, initiated discussion revolving around security of privacy of individuals. The question is why there is threat to privacy of individuals? To answer it, first we need to understand the concept of Digital world or Cyberspace.<sup>2</sup> Digital world or cyberspace is a virtual world which is created by human being which consists of communication device, computer, computer system, computer network, data, computer database or software.<sup>3</sup> In physical world we know what are we doing and what will be consequences of our activities, in contrast to it in virtual world people are not competent to understand the whole process of technology and consequences of their activities. Computer system and internet are easily accessible therefore it is vulnerable platform for people.

## II. INTERNATIONAL INSTRUMENTS PERTAINING TO INFORMATION TECHNOLOGY AND RIGHT TO PRIVACY

Significant international instruments on cyber-space are United Nations Commission on International Trade Law (UNCITRAL) and Cyber Crime Convention (widely known as Budapest convention). Budapest convention is considered as only legally binding international multilateral treaty on cyber- crime.<sup>4</sup>

Right to privacy has been internationally recognised under the Universal Declaration of Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17) and many other relevant treaties.<sup>5</sup>

---

<sup>2</sup> KARUN SANJAYA, Right to Privacy in Cyberspace: An Illusion? Gen Z and Human Rights pp. 254-256, available online at: [https://www.researchgate.net/publication/358285375\\_RIGHT\\_To\\_PRIVACY\\_IN\\_CYBERSPACE\\_-\\_AN\\_ILLUSION](https://www.researchgate.net/publication/358285375_RIGHT_To_PRIVACY_IN_CYBERSPACE_-_AN_ILLUSION) (last accessed on 3<sup>rd</sup> Feb 2022)

<sup>3</sup> The Economic Times, <https://economictimes.indiatimes.com/news/politics-and-nation/india-wins-re-election-to-un-commission-on-international-trade-law/articleshow/49734565.cms?from=mdr> (last visited on Jan. 27, 2022).

<sup>4</sup> WWW.DRISHTIIAS.COM, <https://www.drishtiias.com>, <https://www.drishtiias.com/daily-updates/daily-news-analysis/convention-on-global-cybercrime> (last visited on Jan 28, 2022).

<sup>5</sup> Universal Declaration of Human Rights.

### III. STATISTICS OF CYBER-CRIME

Report on cyber- crime based on the recent survey shows that number of reported cases has been increased by 11.8% in 2020 in comparison to the year 2019.<sup>6</sup> According to the National Crime Records Bureau (NCRB) the rate of cyber -crime (incidents per lakh population) also jumped from 3.3% in 2019 to 3.7% in 2020 in the country. 8578 cases were reported for fake news on social media, 972 related to cyber stalking or bullying of women and children, 149 incidents of fake profile. 3,293 cases relating to sexual exploitation and 2,440 cases relating to extortion were recorded in the year 2021.<sup>7</sup> Despite India has separate legislation to control cyber-crime but there is implementational loophole in it.

### II. LEGAL FRAMEWORK FOR COMBATING CYBER-CRIME IN INDIA

Interchange of information over electronic media has been adopted as an alternate way to paper based traditional communication and storage of information. Since last ten decade, India has witnessed massive increase in usage of internet and electronic devices. Cyber space has been used as a potential medium for committing crime by criminals. Therefore, to regulate activities of cybercriminals, Information Technology Act, 2000 (hereinafter mentioned as IT Act) was enacted and it is considered as sole governing legislation relating to digital world. Before discussing the expression cyber security, we need to understand the expressions “data”<sup>8</sup> and “cyber security”.<sup>9</sup> Data is a technical word which simply refers to information, knowledge or facts either being processed or stored in computer irrespective of the fact whether these data are personal or professional. There have been instances where data have been infringed which raised a question that are we protected in digital space? To solve this question, provisions related to cyber security was introduced in the IT Act. Like physical security is essential in society, cyber security is necessary to protect individuals from falling into the trap of cyber criminals. Cyber- criminals can be prevented by adopting strong cyber security measures.

---

<sup>6</sup> THE HINDU, <https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece> (last visited on Jan 25, 2022).

<sup>7</sup> THE HINDU, <https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece> (last visited on Jan 25, 2022).

<sup>8</sup> Information Technology Act, 2000, § 2(o), No.2, Acts of Parliament, 1949, 2000 (India).

<sup>9</sup> Information Technology Act, 2000, § 2(nb), No.2, Acts of Parliament, 1949, 2000 (India).

An expert committee was constituted to bring amendment in Information Technology Act, 2000, therefore IT (Amendment) Act, 2008 was introduced. Imprisonment and Pecuniary punishment both were enhanced by this Amendment Act but more focus was given to increase pecuniary punishment. Lacuna in process of delivering justice is twofold Firstly, it is difficult to catch cyber criminals, and secondly even if they are caught, they are not punished adequately. The quantum of punishment is not sufficient to prevent or prohibit cyber-crimes.

Rising number of cases of unauthorised access to computer or computer system and encroachment on personal data but unfortunately there is no specific provision which can distinguish 'personal data' and 'sensitive personal data'.<sup>10</sup>

There is dire need of enacting separate legislation which specifically deals with rules and regulations of protecting data. Therefore, there is threat over data protection regime, the government has proposed the Draft on Personal Data Protection Bill, 2018 (based on the recommendation of Justice B.N. Srikrishna Committee) but this legislation has not been enacted by the legislature and it is believed that this legislation would prove to be effective to punish criminals.<sup>11</sup>

#### IV.KINDS OF CYBER CRIME

Statistics of cyber-crime shows drastic increase in number of cyber-crime cases. Cyber-crime has been differentiated on the basis of its nature and some of them are discussed hereafter:

**Harassment via E-mails:** Harassment via E-mails is generally a type of stalking over internet where recipient finds electronic message as offensive or threatening. These types of e-mail contain elements which infringe privacy of victim and affects their mental health.<sup>12</sup>

---

<sup>10</sup> KARUN SANJAYA, Right to Privacy in Cyberspace: An Illusion? Gen Z and Human Rights pp. 254-256, available online at: [https://www.researchgate.net/publication/358285375\\_RIGHT\\_To\\_PRIVACY\\_IN\\_CYBERSPACE\\_-\\_AN\\_ILLUSION](https://www.researchgate.net/publication/358285375_RIGHT_To_PRIVACY_IN_CYBERSPACE_-_AN_ILLUSION) (last accessed on 3rd Feb 2022).

<sup>11</sup> PRSINDIA, <https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018> (last visited on Jan 29,2022).

<sup>12</sup> THE HINDU, <https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece> (last visited on Jan 25,2022).

**Cracking:** It is technique which is used to decode computer or computer system for stealing data and using this data to commit crime against their target.<sup>13</sup>

**Cyber- Stalking:** When a conversation through electronic means is used to threaten or harass or intimidate another individual over internet is cyber stalking. It is extended form of cyber bullying.<sup>14</sup>

**Hacking:** When an unauthorised user usually a cyber-criminal illegally access computer or computer system with the aim of data theft is called as hacking. Hackers are technically sound and they modify coding of computer or computer system easily and use these data or information for making profit.<sup>15</sup> Section 66 of the IT Act deals with the offence of computer hacking. As per Section 66, a person with the intention to cause or with the knowledge that he will cause wrongful loss or damage to the public or any person who destroys or deletes or alters any information residing in computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking.<sup>16</sup> Punishment for committing hacking is imprisonment up to three years or fine which may extend to two lakh Rupees or both.

**Dissemination of obscene materials:** Dissemination of obscene materials is prohibited in any form whether in online mode or in offline mode. Section 67 of Information Technology Act, 2000 prohibits distribution of obscene materials over internet shall be punishable with an imprisonment which may extend to five years and with fine which may extend to ten lakh rupees and in the case of subsequent conviction, imprisonment shall extend to seven years and also with fine which may extend to ten lakh rupees.<sup>17</sup>

**Spoofing:** Spoofing is a type of scam in which a criminal sends an email address, display name, phone number, text message, or website URL to convince a target that they are interacting with a known, trusted source. Spoofing often involves changing just one letter, number, or symbol of the communication so that it looks safe at a quick glance. For example,

---

<sup>13</sup> MY LAW QUESTIONS, <https://www.mylawquestions.com/what-is-email-harassment> (last visited on Jan 27,2022)

<sup>14</sup> [HTTPS://WWW.AVAST.COM](https://www.avast.com), <https://www.avast.com/c-cracking#gref> (last visited on Jan 27,2022).

<sup>15</sup> VERY WELL MIND, <https://www.verywellmind.com/what-is-cyberstalking-5181466> (last visited on Jan 27, 2022)

<sup>16</sup> KARNIKA SETH.COM, <http://www.karnikaseth.com/cybercrimes-defined-under-the-indian-it-act2000.html> (last visited on Jan 28,2022)

<sup>17</sup> Information Technology Act, 2000, § 67, No.2, Acts of Parliament, 1949, 2000 (India)

you could receive an email that appears to be from Netflix using the fake domain name “netffix.in.”<sup>18</sup>

**Page jacking:** Page-jacking involves using the same key words or web site descriptions of a legitimate site on a fake site. If users click on the bogus site, they are frequently led to a pornographic site.<sup>19</sup>

**Carding:** Criminals collect card details of consumers and make phone calls to customers on name of bank employee and if customer gives his bank details, then they withdraw money from their account. As per section 66C Carding is an offence three years of imprisonment or a fine which may extend to one lakh rupees.<sup>20</sup>

Undoubtedly, creation of cyberspace is boon to mankind but it has brought new challenges in the form of cybercrime. Cyberspace is a separate universe from physical world therefore the modus operandi is completely different. Cyber criminals easily take away our personal information without our permission whether it is money transfer or stealing of our personal details. Virtual mode saves time but has taken away our most precious aspect of life that is privacy.

## V. RELATION BETWEEN RIGHT TO PRIVACY AND CYBER CRIME

Despite human beings live in a social life but it is inherent in nature of human beings to keep personal things private. Right to Privacy is a significant facet of leading a dignified life. The right to privacy has been elevated to the status of fundamental right after K.S. Puttuswamy judgment.<sup>21</sup> Before the judgment of K.S. Puttuswamy right to privacy was considered as a ‘penumbral right’ which means that a right which is recognised by the Supreme Court as part to the fundamental right to life and liberty. The first case which discussed privacy as a right was Maneka Gandhi v. Union of India.<sup>22</sup> In Maneka Gandhi’s case Supreme Court observed that right to life also include right to live with human dignity. In Francis Coralie v. Union Territory of Delhi,<sup>23</sup> the Court declared that “The right to life includes the right to live with human dignity and all that goes along with it, viz., the bare

---

<sup>18</sup> INVESTOPEDIA, <https://www.investopedia.com/terms/s/spoofing.asp> (last visited on Jan 29, 2022).

<sup>19</sup> LAW.JRANK.ORG, <https://law.jrank.org/pages/11984/Cyber-Crime-Page-Jacking> (last visited on Jan 29, 2022).

<sup>20</sup> INVESTOPEDIA.COM, <https://www.investopedia.com/terms/c/carding> (last visited on Jan 29, 2022)

<sup>21</sup> K.S. Puttuswamy v. Union of India, 2017 10 SCC 1.

<sup>22</sup> Maneka Gandhi v. Union of India, AIR 1978 SC 597.

<sup>23</sup> Francis Coralie v. Union Territory of Delhi, AIR 1981 SC 746.

necessities of life such as adequate nutrition, clothing and shelter over the head and facilities for reading writing and expressing oneself in diverse forms, freely moving about and mixing and mingling with fellow human beings and must include the right to basic necessities of life and also the right to carry on functions and activities as constitute the bare minimum expression of human self.”<sup>24</sup> Next landmark judgment in development of right to privacy as a fundamental right was *Kharak Singh v. State of UP*, the majority judges concluded that the under the Constitution of India right to privacy is not a express and separate right and it further held that an unauthorised intrusion into a person’s house and disturbances caused to him is violation of essential freedom of leading a peaceful private life. Justice Subba Rao’s judgment is considered by jurists as landmark judgment which formed right to privacy as a separate fundamental right. He observed that right to life and liberty is not limited only to live a life free from restrictions imposed on movements but also freedom from intrusion into his personal life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person’s house, where he lives with his family, is his ‘castle’; it is his rampart against encroachment on his personal liberty.”<sup>25</sup> In *Govind v. State of Madhya Pradesh*,<sup>26</sup> the Court declared that right to privacy derives its origination from Article 19(1) (a), (d) and 21 but its scope is limited. In another judgment *PUCL v. Union of India* <sup>27</sup> the Court ruled that “right to privacy is a part of the right to ‘life’ and ‘personal liberty’ enshrined under Article 21 of our Constitution. Judgment in *PUCL v. Union of India*<sup>28</sup> the right to privacy has been expressly declared by the Supreme Court but it was concretised by the judgment of *K.S. Puttuswamy v. Union of India*. Bench of nine judges unanimously overruled the decisions of *M.P. Sharma* and *Kharak Singh* and declared that right to privacy as fundamental right within Article 21 in particular and Part III as whole. After this judgment, right to privacy has been given constitutional position. After the judgment of *K.S. Puttuswamy* right to privacy became fundamental right hence the breach of data amounts to infringement of individual’s fundamental right.

---

<sup>24</sup> Francis Coralie v. Union Territory of Delhi, AIR 1981 SC 746.

<sup>25</sup> *Kharak Singh v. State of UP*, AIR 1963 SC 1295.

<sup>26</sup> *Govind v. State of Madhya Pradesh*, AIR 1963 SC 1295.

<sup>27</sup> *PUCL v. Union of India*, AIR 1997 SC 568.

<sup>28</sup> *PUCL v. Union of India*

Dimensions of privacy has changed in digital space, securing citizens' privacy on internet is a challenge for government. One's personal life can be encroached anytime by anonymous person. There has been rapid growth in the development of software application whether in gaming or business or social media application like Instagram, Facebook or tik tok where an individual has to give their basic information before availing access to the application. Installation of various applications, sharing or uploading photos or messages through social media have become part of day-to-day life. Whenever anyone downloads any application, that person shares his personal details with the company of Application but problem arises when people share private information or photos or anything private with someone over social media platform then that data is also shared with the App's company; that particular company is entrusted to keep it private but practically this is not so. Sometimes data are hacked or it is also sold on dark web. Punishment for violating individuals' privacy is imprisonment for three years or with fine not exceeding two lakh rupees, or with both.<sup>29</sup> In present techno-savvy world avoidance of computer or internet use is not possible therefore there is requirement of strengthening security measures in cyber-space.

---

<sup>29</sup> Information Technology Act, 2000, § 66E, No.2, Acts of Parliament, 1949, 2000 (India).



## VI. CONCLUSION AND SUGGESTIONS

Generically, cyber-criminals and hackers are more technically advanced than those who are active or regulating social media platforms. People have become more efficient technologically but government bodies are not efficient and the legislations enacted by the government is also not in consonance with the present time. Privacy of individuals has been compromised in digital era although legislations have been enacted to combat with cyber-crime but statistics of cyber- crime is increasing every year. Information Technology (Amendment) Act, 2008 inserted strict penal provisions but it has not been proved effective, Government of India should adopt more effective measures to regulate virtual world. Another issue is lack of technical knowledge; people don't have technical knowledge; majority of population are active on internet without having practical knowledge.

To overcome abovementioned loopholes of IT Act and to combat the cyber challenges suggestions are hereinafter put forth:

1. Awareness is the best measure which can combat cyber- crime. Government should take active steps to aware people in this field so that would help in decreasing the number of cases.
2. Effective hierarchy of tribunals must be established to deal with the new challenges of cyber space.
3. A robust and comprehensive data protection law shall be set up which shall be regulated by the technically efficient persons.
4. Recommendations of ISO/IEC shall be made mandatory for every public/private institution.
5. There is urgent need of enacting comprehensive data protection legal framework to make it more effective.
6. All cyber- crime shall be made non-bailable offence under the IT Act, 2000.