Page 2153 - 2170

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 4

2020

Cybercrimes in the Social Media Issues and Challenges

DEBASREE DEBNATH[1]

ABSTRACT

Cybercrimes use the computers, internet, human behaviour and other technology based mediums for the criminal misconduct. In the contemporary era, the technology-based devices help to increase the computer perpetrated crimes in the society; these crimes exist more stringently as it is difficult to apprehend the criminals. It becomes easy for the perpetrators to commit such crimes in today's era as globalization has gifted us the fastest internet infrastructure facility at very low cost. Social media has become the part and parcel of everyone's life, irrespective of the age group which is affecting the lives of the individuals, as these people share a lot of their personal and social life in the media through Facebook, Instagram and WhatsApp. It becomes a challenge for the intelligence bureau to catch the cyber criminals because, firstly, these criminals use the internet very cleverly commit the crimes and secondly, due to the ongoing technological developments which provides them platform for committing such crimes. These people are using internet as a tool and getting the information which is available in the pool of social media as well as other internet sources for committing the crime which in turn are violating the right to privacy of an individual. The criminals by using the digital communication channel hack the user and company profiles, and then they sell the stolen identities for their illegal gains. The RSA Anti-Fraud Command Center reported that, 43 percent fraud attacks were increased in the 2018 as the cyber criminals are finding new ways to exploit the social media. The researcher in this paper discussed the various ongoing cybercrimes on social media and need to harmonise the legal aspects of cyber security. The researcher also tried to discuss the measures for protection of individual's rights from social networking sites and how they need to protect their data in the social media platform.

Keywords: *Cybercrime, Social Media, Technological Advancement, Cyber Security, Privacy.*

I. INTRODUCTION

The concept of privacy has played a large role in legal discussions and judgments during the last century all over the world including India. Privacy is understood in this context as "liberty or freedom to act in personal matters". To understand better how the concept of privacy is philosophically connected in constitutional law we have lots of precedents all over the world

[1] Author is a PhD Scholar and Research Associate at Maharashtra National Law University, Nagpur

 [ISSN 2581-5369]

by constitutional courts. Data protection is a necessity, it becomes more obvious when the amount of data created and stored continues to grow at an unprecedented rate, coupled with exploitation and mishandling of such data by tech companies and giant service providers e.g. Google, Amazon and other social networking websites and digital service providers without the consent of the individual. The right to privacy is widely acknowledged and well-supported in civilized countries including India and the United States. Many familiar legal and ethical arguments pivot on an appeal to the right to privacy. A charge that a government, a corporation, or an individual has invaded someone's privacy is regarded as a serious matter. The concept of privacy seems so obvious, so basic, and so much a part of our social values, that there may seem to be little room for any philosophical misgivings about it. However, substantial philosophical controversy about the nature of privacy exists. The philosophical debate focuses largely on two major questions: What is privacy? and Can the right to privacy be philosophically justified?[2]

This paper will try to answer these questions as well as all other questions related to this. To safeguard the data available with various agencies, and to curb the trade in data without the user's consent, the Personal Data Protection (PDP) Bill was drafted. This Bill was introduced in the Lok Sabah on December 11, 2019, and pending before the Joint Parliamentary Committee for scrutiny. This Bill was introduced with a futuristic aim to protect the personal data of the individual, to lays down the guidelines and rules for the utilization of data, and to the established data protection authority. In recent, the litigation history of the data protection regime in India can be formally traced back to the petition filed before the Hon'ble Supreme Court by Retired Justice K.S. Puttaswamy. The court has in its a landmark judgment held that *the right to privacy* is protected as

"an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution"[3].

In **K.S. Puttaswamy v Union of India**[4], the Court read the right to privacy to be a fundamental right but with reasonable restrictions, such as

2 James H. Moor, *The Ethics of Privacy Protection*, (June 2, 2020) https://www.researchgate.net/publication/32961262_The_Ethics_of_Privacy_Protection?enrichId=rgreq9be4abcf1cf8a9d3fe07f736fd6225c2XXX&enrichSource=Y292ZXJQYWdlOzMyOTYxMjYyO0FTOjEwMzA5NTQ2Mzg0MTc5N0AxNDAxNTkxMjgyODE5&el=1_x_2&_esc=publicationCoverPdf

3 Jyoti Panday, *India's Supreme Court Upholds Right to Privacy as a Fundamental Right—and It's About Time*, DEEPLINK BLOG, (June 2, 2020). https://www.e.org/deeplinks/2017/08/indias-supreme-court-upholds-rightprivacy-fundamental-right-and-its-about-time.

4 (2017) 10 SCC 641

 [ISSN 2581-5369]

(i) existence of law (ii) legitimate state aim (iii) proportionality.[5]

According to the judgment, the Supreme Court also directed the government to form a data protection law to address the concerns related to privacy in the digital age.

A committee of experts headed by the Justice B.N. Srikrishna, was set up to assess the current scenario of data protection in India, recommend ways to tackle the problems surrounding it and draft a data protection bill, a bill was presented in the year 2018 but after various criticism bill was later presented in 2019 again. This time Bill includes several modifications and changes in scope and intent for creating a framework for "organizational and technical measures" of data processing, introduce "accountability of entities processing personal data", and lay down norms for social media intermediaries and cross border transfer[6].

II. THE CONCEPT OF PRIVACY: A PHILOSOPHICAL LOOK

The concept of privacy has been analyzed extensively by contemporary philosophers. Philosophers, like everyone, have been struck by the broad dissemination and the forceful impact of information technology during the last few decades. Therefore, it is not surprising that most contemporary philosophical accounts of privacy tie it closely to the concept of information. Although control of information is an aspect of privacy, these definitions emphasizing control are inadequate for there are many situations in which people have no control over the exchange of personal information about themselves but in which there is no loss of privacy. Consider some examples[7] Philosophers have offered a variety of justifications of privacy as an important value. Stanley Benn suggests that privacy is grounded in respect for persons. As Benn puts it: "To respect someone as a person is to concede that one ought to take account of how his enterprise might be affected by one's own decisions." This type of justification for privacy is both popular and at least initially plausible. One problem with giving respect for persons as a justification for privacy is that it does not distinguish between times in which privacy is justified and times in which it is not. Apart from PDP Bill, 2019 we have some other laws and regulations to answer the issue related to privacy that are

III. PRESENT REGULATORY FRAMEWORK

In absence of a dedicated data protection legislation India is trying to answer the problems related to this issue by using available law and regulation enacted time to time to answer these

5 Sinha Amber, *comments to the personal data protection Bill 2019*, THE CENTRE FOR INTERNET & SOCIETY (CIS), (June 2, 2020). https://cis-india.org/internet-governance/blog/comments-to-the-personal-data-protection-Bill-2019.
6 The Personal Data Protection Bill,2019, s. 26 & 33.
7 Ibid 1

 [ISSN 2581-5369]

type of problem, we will try to evaluate the available laws, rules, and regulation and will also assess the usefulness of these laws, this study will help to disclose whether we need a new law especially dedicated to protecting the personal data and privacy of an individual or the available legislation and provisions are sufficient in this regard.

A. PRIVACY AND DATA PROTECTION LEGISLATION

In the absence of specific legislation, data protection is achieved in India through the enforcement of privacy rights based on a patchwork of legislation, as follows.

(i) THE INFORMATION TECHNOLOGY ACT (2000) (IT ACT) AND THE INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008[8]

The IT Act contains provisions for the protection of electronic data. The IT Act penalizes 'cyber contraventions' (Section 43(a)–(h)), which attract civil prosecution, and 'cyber offenses' (Sections 63–74), which attract criminal action.

The IT Act was originally passed to provide legal recognition for e-commerce and sanctions for computer misuse. However, it had no express provisions regarding data security. Breaches of data security could result in the prosecution of individuals who hacked into the system, under Sections 43 and 66 of the IT Act, but the Act did not provide other remedies such as, for instance, taking action against the organization holding the data. Accordingly, the IT (Amendment) Act 2008 was passed, which, inter alia, incorporated two new sections into the IT Act, Section 43A and Section 72A, to provide a remedy to persons who have suffered or are likely to suffer a loss on account of their personal data not having been adequately protected.

(ii) THE INFORMATION TECHNOLOGY RULES (THE IT RULES)

Under various sections of the IT Act, the government routinely gives notice of sets of Information Technology Rules to broaden its scope. These IT Rules focus on and regulate specific areas of collection, transfer, and processing of data, and include, most recently, the following:

a. the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules,[9] which require entities holding users' sensitive personal information to maintain certain specified security standards;

[8] IT Act and Rules (Aug 12, 2020) meity.gov.in/content/cyber-laws.
[9] meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.

 [ISSN 2581-5369]

b. the Information Technology (Intermediaries Guidelines) Rules,[10] which prohibit content of a specific nature on the internet, and an intermediary, such as a website host, is required to block such content;

c. the Information Technology (Guidelines for Cyber Cafe) Rules,[11] which require cybercafés to register with a registration agency and maintain a log of users' identities and their internet usage; and

d. the Information Technology (Electronic Service Delivery) Rules,[6] which allow the government to specify that certain services, such as applications, certificates, and licenses, be delivered electronically.

The IT Rules are statutory law, and the four sets specified above were notified on 11 April 2011 under Section 43A of the IT Act.

Penalties for non-compliance are specified by Sections 43 and 72 of the IT Act.

The IT Rules define personal information as any information that relates to a natural person that, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.

Further, the IT Rules define 'sensitive personal data or information' as personal information consisting of information relating to:

a. passwords;

b. financial information, such as bank account, credit card, debit card or other payment instrument details;

c. physical, physiological and mental health conditions;

d. sexual orientation;

e. medical records and history;

f. biometric information;

g. any details relating to the above clauses as provided to a body corporate for the provision of services; or

h. any information received under the above clauses by a body corporate for processing, or that has been stored or processed under lawful contract or otherwise.

[10] meity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf.
[11] meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.

 [ISSN 2581-5369]

Provided that any information is freely available or accessible in the public domain, or furnished under the Right to Information Act 2005 or any other law for the time being in force, it shall not be regarded as sensitive personal data or information for these rules.

B. ADDITIONAL LEGISLATION

In addition to the legislation described above, data protection may also sometimes occur through the enforcement of property rights based on

1. the Copyright Act (1957)
2. the Code of Criminal Procedure (1973)
3. the Indian Telegraph Act 1885
4. the Companies Act (2013)
5. the Competition Act (2002)
6. the Consumer Protection Act (2019) in cases of unfair trade practices are also relevant

Finally, citizens may also make use of the common law right to privacy, at least in theory – there is no significant, recent jurisprudence on this.[12]

C. COMPLIANCE REGULATORS

(i) CERT-IN

Under Section 70B of the IT (Amendment) Act 2008, the government constituted CERT-In, which the website of the Ministry of Electronics and Information Technology refers to as the 'Indian Computer Emergency Response Team'. CERT-In is a national nodal agency responding to computer security incidents as and when they occur. The Ministry of Electronics and Information Technology specifies the functions of the agency as follows:

a. collection, analysis, and dissemination of information on cybersecurity incidents;

b. forecast and alerts of cybersecurity incidents;

c. emergency measures for handling cybersecurity incidents;

d. coordination of cybersecurity incident response activities; and

e. issuance of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response to and reporting of cybersecurity incidents.[7]

12 Aditi Subramaniam & Sanuj Das, The Privacy, Data Protection and Cybersecurity Law Review - Edition 6 ,218, (June 22, 2020) https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210048/india

 [ISSN 2581-5369]

(ii) CYBER REGULATIONS APPELLATE TRIBUNAL (CRAT)

Under Section 48(1) of the IT Act 2000, the Ministry of Electronics and Information Technology established CRAT in October 2006. The IT (Amendment) Act 2008 renamed the tribunal Cyber Appellate Tribunal (CAT). Under the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities, or by an adjudicating officer under this Act, may prefer an appeal before the CAT. The CAT is headed by a chairperson who is appointed by the central government by notification, as provided under Section 49 of the IT Act 2000.

Before the IT (Amendment) Act 2008, the chairperson was known as the presiding officer. Provisions have been made in the amended Act for CAT to comprise of a chairperson and such several other members as the central government may notify or appoint.[8]

D. SPECIFIC REGULATORY AREAS

1. FINANCIAL PRIVACY

i) PUBLIC FINANCIAL INSTITUTIONS (OBLIGATION AS TO FIDELITY AND SECRECY) ACT 1983[13]

Under this Act, public financial institutions are prohibited from divulging any information relating to the affairs of their clients except by laws of practice and usage.

ii) THE PREVENTION OF MONEY LAUNDERING ACT 2002[14]

The Prevention of Money Laundering Act (PMLA) was passed in an attempt to curb money laundering and prescribes measures to monitor banking customers and their business relations, financial transactions, verification of new customers, and automatic tracking of suspicious transactions. The PMLA makes it mandatory for banking companies, financial institutions and intermediaries to furnish to the Director of the Financial Intelligence Unit (under the PMLA) information relating to prescribed transactions, and which can also be shared, in the public interest, with other government institutions or foreign countries for enforcement of the provisions of the PMLA or through exchanges of information to prevent any offense under the PMLA.

iii) CREDIT INFORMATION COMPANIES (REGULATION) ACT 2005 AND THE CREDIT INFORMATION COMPANIES REGULATIONS 2006[15]

This legislation is essentially aimed at the regulation of sharing and exchanging credit

[13]http://lawmin.nic.in/ld/PACT/1983/The%20Public%20Financial%20Institutions%20(Obligation%20as%20to%20Fidelity%20and%20Secrecy)%20Act,%201983.pdf.
[14] http://fiuindia.gov.in/pmla2002.htm.
[15] www.cibil.com/sites/default/files/pdf/cicra-act-2005.pdf.

 [ISSN 2581-5369]

information by credit agencies with third parties. Disclosure of data received by a credit agency is prohibited, except in the case of its specified user and unless required by any law in force.

The regulations prescribe that the data collected must be adequate, relevant, and not excessive, up to date and complete, so that the collection does not intrude to an unreasonable extent on the personal affairs of the individual. The information collected and disseminated is retained for a period of seven years in the case of individuals. Information relating to criminal offenses is maintained permanently while information relating to civil offenses is retained for seven years from the first reporting of the offense. The regulations also prescribe that personal information that has become irrelevant may be destroyed, erased, or made anonymous.

Credit information companies are required to obtain informed consent from individuals and entities before collecting their information. For redressal, a complaint can be written to the Reserve Bank of India.

iv) PAYMENT AND SETTLEMENT SYSTEMS ACT 2007[16]

Under this Act, the Reserve Bank of India (RBI) is empowered to act as the overseeing authority for the regulation and supervision of payment systems in India. The RBI is prohibited from disclosing the existence or contents of any document or any part of any information given to it by a system participant.

v) FOREIGN CONTRIBUTION REGULATION ACT 2010[17]

This Act is aimed at regulating and prohibiting the acceptance and utilization of foreign contributions or foreign hospitality by certain individuals, associations or companies for any activities detrimental to the national interest and, under the Act, the government is empowered to call for otherwise confidential financial information relating to foreign contributions of individuals and companies.

2. WORKPLACE PRIVACY

In the present scenario, employers are required to adopt security practices to protect sensitive personal data of employees in their possession, such as medical records, financial records, and biometric information. In the event of a loss to an employee due to lack of adequate security practices, the employee would be entitled to compensation under Section 43A of the Information Technology Act 2000. Other than this piece of legislation, there is no specific legislation governing workplace privacy, although, concerning the workplace, the effect of the

[16] https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf.
[17] https://fcraonline.nic.in/home/PDF_Doc/FC-RegulationAct-2010-C.pdf.

 [ISSN 2581-5369]

Supreme Court judgment on privacy as a fundamental right remains to be seen.

3. CHILDREN'S PRIVACY

Section 74 of the Juvenile Justice (Care and Protection of Children) Act 2015 mandates that the name, address or school, or any other particular, that may lead to the identification of a child in conflict with the law or a child in need of care and protection or a child victim or witness of a crime shall not be disclosed in the media unless the disclosure or publication is in the child's best interest.

4. HEALTH AND MEDICAL PRIVACY

Under the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (Code of Ethics Regulations 2002)[18] regulations, physicians are obliged to protect the confidentiality of patients during all stages of procedures, including information relating to their personal and domestic lives unless the law mandates otherwise or there is a serious and identifiable risk to a specific person or community of a notifiable disease.

i) MEDICAL TERMINATION OF PREGNANCY ACT 1971

This Act prohibits the disclosure of matters relating to treatment for termination of pregnancy to anyone other than the Chief Medical Officer of the state. The register of women who have terminated their pregnancy, as maintained by the hospital, must be destroyed on the expiry of a period of five years from the date of the final entry.

ii) ETHICAL GUIDELINES FOR BIOMEDICAL RESEARCH ON HUMAN SUBJECTS

These Guidelines require investigators to maintain the confidentiality of epidemiological data. Data of individual participants can be disclosed in a court of law under the orders of the presiding judge if there is a threat to a person's life, allowing communication to the drug registration authority in cases of severe adverse reaction and communication to the health authority if there is a risk to public health.

E. GENERAL OBLIGATIONS FOR DATA PROCESSORS, CONTROLLERS, AND HANDLERS IN PRESENT SYSTEM

The IT Rules provide certain obligations to data processors, Controllers, and Handlers of the data of citizens, these obligations are must create a relationship between data principle and other authorities, the PDP Bill also provide certain provisions of same nature with updated

[18] http://niti.gov.in/writereaddata/files/1.pdf

 [ISSN 2581-5369]

views

(i) TRANSPARENCY

The IT Rules state that all data handlers must create a privacy policy to govern the way they handle personal information. Further, the policy must be made available to the data subject who is providing this information under a lawful contract.

(ii) LAWFUL BASIS FOR PROCESSING

A body corporate (or any person or entity on its behalf) cannot use data for any purpose unless it receives consent in writing from the data subject to use it for that specific purpose. Consent must be obtained before the collection of the data. The IT Rules also mandate that sensitive personal information may not be collected unless it is connected to the function of the corporate entity collecting it, and then only if the collection is necessary for that function. It is the responsibility of the body corporate to ensure that the sensitive personal information thus collected is used for no other purpose than the one specified.

(iii) PURPOSE LIMITATION

Neither the IT Rules nor the IT Act specifies a time frame for the retention of sensitive personal information. However, the IT Rules state that a body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(iv) DATA RETENTION

Section 67C of the IT Act requires that an intermediary preserve and retain information in a manner and format and for such a period as prescribed by the central government.

(v) REGISTRATION FORMALITIES

India currently does not have any legislative requirements for registration or notification procedures for data controllers or processors, and it is a great lacuna in the eye of the law.

F. RIGHTS OF INDIVIDUALS IN PRESENT SYSTEM

(i) ACCESS TO DATA

Rule 5, Subsection 6 of the IT Rules mandates that the body corporate or any person on its behalf must permit providers of information or data subjects to review the information they may have provided.

(ii) Correction and deletion

 [ISSN 2581-5369]

Rule 5, Subsection 6 of the IT Rules states that data subjects must be allowed access to the data provided by them and to ensure that any information found to be inaccurate or deficient shall be corrected or amended as feasible. Although the Rules do not directly address deletion of data, they state in Rule 5, Subsection 1 that corporate entities or persons representing them must obtain written consent from data subjects regarding the usage of the sensitive information they provide. Further, data subjects must be provided with the option not to provide the data or information sought to be collected.

The Supreme Court of India in a nine-judge bench decision in August 2017 in *KS Puttaswamy & Ors v. Union of India & Ors*[19]also identified the right to be forgotten, in physical and virtual spaces such as the internet, under the umbrella of informational privacy.

(iii) Objection to processing and marketing

Rule 5 of the IT Rules states that the data subject or provider of information shall have the option to later withdraw consent that may have been given to the corporate entity previously, and the withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the corporate body is prohibited from processing the personal information in question. In the case of the data subject not providing consent, or later withdrawing consent, the corporate body shall have the option not to provide the goods or services for which the information was sought.

(iv) Right to restrict processing

pro Crime has its genesis in various factors which can be traced into various social, economical and institutional aspects. In the era of globalisation, crime ratio is much higher than the previous era, as today the internet has also become a threat to everyone which we use in our daily life. Cybercrime is a kind of crime that is committed though a computer and by using computer network. There are various types of Cybercrime such as identity thefts, phishing scams, cyber stalking, online harassment. The social media has become an easy platform for the cyber criminals for collecting the information of an individual. Online harassment, hacking of profiles, email spoofing, SMS spoofing are said to be quite common now-a-days. There have been quite a lot of cases where all these activities have led to people being traumatized. In some worst-case scenarios people have lost their lives too. Rapid change in the technology, lack of awareness about the anti-malware and anti-virus software, lack of transparency by the social media and unable to tackle the unauthorised use of social media are the major reasons for the cybercrimes on social media. The legislature and judiciary are working hard to prohibit such

[19] http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

 [ISSN 2581-5369]

kind of activities and to protect the privacy of an individual. Cybercrimes can be avoided if we report against the suspicious activities and limiting ourselves to known people. The researcher in this paper discussed the various types of cybercrimes on social media and how it violates the individual's right to privacy.

IV. SOCIAL MEDIA AND CYBERCRIMES

Social media becomes the hub of cybercrimes in the present era. The cyber criminals find it very easy to victimise the individual using the data available in the internet. The lack of skilled and trained manpower to tackle the cyber criminals at the initial level are one of the main reasons of the increasing ratio of cybercrimes in India. The cyber criminals generally can hide themselves as it is very easy for them to do so. Therefore, it requires a proper intelligence bureau to catch the cyber criminals.

Hacking

Hacking is a more common form of cybercrime known till date. In hacking the cyber criminals use the computer system in an unauthorised manner and destroy the computer programmes and data available in the computer system. The most dreadful thing in hacking is the victim did not know about the hacking activity and the hacker without the knowledge of the victim steal all the confidential data and tempered with it.

Social media platforms are remunerative targets for cybercriminals these days due to the enormous amounts of personally identifiable information that they gather and store from their users.

Hackers always look for different tools and platforms to exploit vulnerabilities on these social media platforms to steal user's personal identifiable information (PII). One of the Social media giant Facebook on September 25, 2018 published that their engineering team had discovered, hackers had exploited vulnerability in their code. The attackers exploited the security flaws in Facebook's "View As" code; it is a feature which helps the users to see how their own Facebook profile looks like to the other Facebook users or to the public in general. Facebook said the stolen tokens were digital keys which were used to take over people's accounts.

In the month of July, 2017 for the first time the vulnerability in Facebook's code was first appeared; it is when they made a change in video uploading feature. Facebook didn't noticed any suspicious activity until September 14, 2018, when there was a sudden jump in user's access to the site. After this Facebook launched a thorough investigation into the suspicious behaviour and discovered this attack. So, attackers had a total of 14 months from July 2017 to

 [ISSN 2581-5369]

September 2018, to exploit the vulnerability in Facebook's code.

Facebook earlier said it has reset access tokens for nearly 50 million user accounts that were supposedly affected and another 40 million user accounts that were subjected to "View As" look up. However, in its latest statement they revealed hackers actually stolen access for 30 million user accounts and gained complete access to user's profiles.

The vulnerability in Facebook's code was later fixed in September 2018, it alerted and apologised to users. Those users had to log back in to their Facebook account, including any of their apps like Hotstar, Zomato which use Facebook login. Once they logged in, they got notification at the top of their News Feed explaining what happened. At last Facebook turned off their "View As" feature temporarily.

Recently, 'FireEye'-a cyber security firm located in US reported that, the hackers succeeded in breaking one of the healthcare website which is situated in India and stolen sixty-eight lakh records which contain the information of the patients and doctors. The firm also mentioned that, cyber criminals were directly selling the data which they stole from healthcare organisations and web portals globally including India in the underground markets; these hackers were mostly belonged from China.[20]

Dissemination of Obscene Material

Various web portal and web sites are used for indecent exposure or pornography using the internet; all these sites contain prohibited and obscene materials which can be harmful for the teenager and adolescent's mind. Cyber stalking includes the sending of obscene and indecent materials to the victim by using the social networking site or through emails or messaging platforms. Section 292 of the Indian Penal Code (IPC) 1860 mentioned about the obscene materials. In addition to section 292 of IPC 1860, the Information Technology Act 2000 under section 67[21] discussed about obscenity as an offence when it is published or transmitted or caused to be published in any electronic form. The Supreme Court in Renjith D. Udeshi v. State of Maharashtra[22] defined the term 'obscenity;' it mentioned that, it means the things which are

[20] IANS, *Hackers Attack Indian Healthcare Website, steal 68 lakh records*, THE ECONOMIC TIMES, Aug. 22, 2019.

[21] Punishment for publishing or transmitting obscene material in electronic form.–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.

[22] A.I.R. 1965 S.C. 881 (India).

 [ISSN 2581-5369]

offensive to modesty or decency; lewd, filthy, and repulsive. Similarly, the Apex Court in Aveek Sarkar v. State of West Bengal[23] decided that, a picture of a nude/semi-nude woman cannot itself be called as obscene except it has the propensity to stir the feelings or revealing an overt sexual desire.

E-Mail and SMS Spamming

Spamming is a very common way of hacking; it is when the same message was send indiscriminately to a huge number of internet users. Cyber criminals now-a-days uses social media platform for spamming. With the rise in several phishing and spamming attack claiming them to be originated from the Income Tax Department, Government of India, recently, the department has issued their list of their all official email-id's, SMS sender Id and even websites used by the taxman to communicate with the tax payer. To avoid any spamming or phishing attempt the Income Tax Department has asked all tax payers to not open any messages from any sender other than the one mentioned in the list. The department of income tax also mentioned that, before you click, always check if the sender is among the listed sources. The department has also asked the tax payers to report any email or SMS or website URL, if they think it is pretending to be of Income Tax Department.

E-Mail and SMS Spoofing

It can be termed as the forgery of an email-id as it misrepresents its origin. Here, the email wrongly shows the intended source and seems to have originated from someone or somewhere other than its actual and true source. It displays the incorrect origin which is different from the source in which it actually originates.

On the other hand, in SMS spoofing the hackers steals the original and authentic identity of the mobile number of an individual and send the SMS by using the internet. The SMS receiver receives the message from that individual person's mobile number who is actually the victim of such kind of spoofing. However, in the present era, Information Technology Act 2000 under section 66C[24] provides the punishment for identity theft.

Cyber Terrorism

In this kind of cyber-crimes the pace and medium is known as the cyberspace; it is usually refers to various actions –simple online propaganda to terrorist attack by using the online

[23] (2014) 4 S.C.C. 257 (India).

[24] Punishment for identity theft - 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.

 [ISSN 2581-5369]

platform. This kind of attacks are pre-planned and used by the cyber criminals for an immense violence in the domain of cybercrime.

Cyber-Stalking

"Cyber stalking" is defined as a crime where the stalkers use internet to commit the crime; they can also use any other electronic device to stalk someone for committing cyber-staling. Here stalkers harass or give threat to the victim repeatedly by using the internet. Section 354D of the Indian Penal Code 1860 defines the term stalking which was added by the 2013 amendment Act.[25] In the year 2017 the National Crime Record Bureau reported that, the total number of cyber-stalking against the women or children is 542.[26]

State	No. of Cases
Maharashtra	301
Andhra Pradesh	48
Haryana	27
Telangana	26
Madhya Pradesh	25
Total India	542

Online Harassment and Trolling

Online harassment is also known as online bullying. These bullying always starts with cyber stalking and then slowly lead to online harassment. Online harassment mostly happens on

[25] Stalking - 1) Any man who—
1. follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
2. monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking;

Provided that such conduct shall not amount to stalking if the man who pursued it proves that—
1. it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or
2. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
3. in the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

[26] Nishtha Vishwakarma, *Cybercrime cases double in 2017, 56% cybercrime cases for fraud motive: NCRB 2017 Report*, MEDIANAMA (July 30, 2020, 5:45 PM), https://www.medianama.com/2019/10/223-cybercrime-ncrb-2017/.

 [ISSN 2581-5369]

social media site such as Facebook, Instagram, and twitter. What happens here is that the perpetrators appear to be friends with the victim at the beginning. The harassments generally start after they gather some information about the victim. Generally, the threats start through emails, messaging services like WhatsApp, Telegram, SMS and so on. Celebrities have millions of followers on their social media account, which sometimes meet with unexpected circumstances, such as bullying or trolling. Now-a-days, cyber criminals troll celebrities on almost every action or event. Such as Sonu Nigam, one of the leading Indian playback singers, in one of the flight used the airline telephone with crew's permission to entertain the passengers by singing a song; after the video clip went viral on social media platforms he was relentlessly trolled for using airline telephone for singing.

Pornography

Pornography is a common cybercrime which prevail in today's society; it usually use in order to cause sexual excitement by using the internet. Pornography refers to pornographic websites, pornographic magazines which are used for sexual excitement by using computer and the internet. It can also be delivered over mobile phones so that the viewer can easily get access to these pornographic websites. Child Pornography is again another threat which involves the use of computer and internet to create and distribute the access of such child pornography to sexually exploit the underage children.

Cybercrime and Breach of Privacy

The fast spreading internet network has growing with the advancement of globalisation which in turn leads to threatening the privacy of an individual. The right to privacy is protected under the legal shield of Article 21 of the Constitution of India as rightly mentioned by the Apex Court in *K. S. Puttaswamy v. Union of India.*[27] Hence, if there is any cybercrime which effect the privacy of an individual then the accused can face the legal hurdles and provide remedy to the victim.

In cybercrimes the hackers violate one's right to privacy and steal the personal information and data of the victim. The hackers steal the intellectual work of the victim while violating the notion of privacy of an individual. Section 66E[28] of Information Technology Act 2000 deals

[27] (2015) 8 S.C.C. 735.

[28] Punishment for violation of privacy–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.

Explanation.–For the purposes of this section–

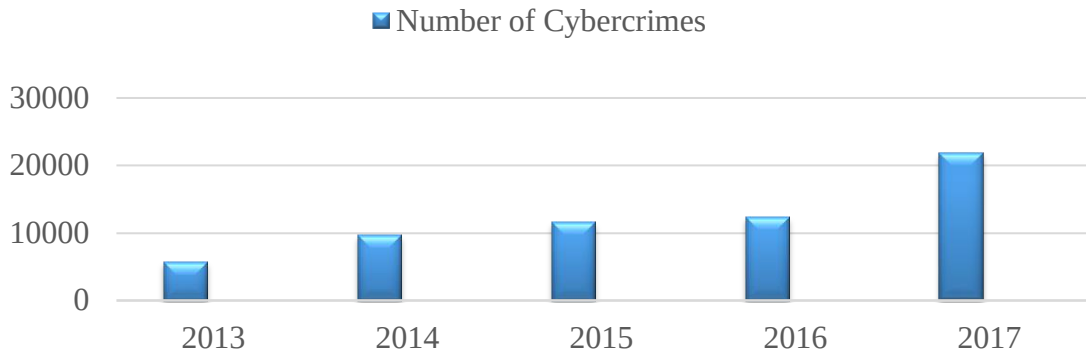
(*a*) —transmit means to electronically send a visual image with the intent that it be viewed by a person or persons;

(*b*) —capture, with respect to an image, means to videotape, photograph, film or record by any means;

with the punishment for violation of privacy. It provides punishment for the cyber criminal who violate the privacy of an individual using the internet.

V. Statistics of Cybercrime in India

Globalisation has an immense impact in the present era. Every one of us, irrespective of the age group uses social media relentlessly and shares our personal data by using Facebook, Instagram and WhatsApp. Social media becomes a hub of personal data of an individual and the cyber criminals by using these data very easily commit the cybercrimes. The term privacy includes the information access without the consent of the individual. The National Crime Record Bureau reported that, in the year 2017 Uttar Pradesh has the highest number of cases on cybercrimes with 4,971 cases followed by Maharashtra (3,604) and Karnataka (3,174).[29] The following chart shows the increasing ratio of cybercrime from 2013 to 2017 in India.[30]



Apart from this, again in the year 2018, the NCRB report mentioned that, 55.2% of cyber-crime cases were registered for the motive of fraud (15,051 out of 27,248 cases) followed by sexual exploitation with 7.5% (2,030 cases) and causing disrepute with 4.4% (1,212 cases).[31]

VI. Conclusion

In the present era the internet has an immense impact on everyone's life as it becomes a part

(*c*) —private area means the naked or undergarment clad genitals, public area, buttocks or female breast:
(*d*) —publishes means reproduction in the printed or electronic form and making it available for public;
(*e*) —under circumstances violating privacy‖ means circumstances in which a person can have a reasonable expectation that–
(*i*) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
(*ii*) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

[29] Sumant Sen, *NCRB Data: Cybercrimes Reached a New High in 2017*, the HINDU, Nov. 05, 2019.

[30] *Ibid.*

[31] National Crime Records Bureau, *Crime in India Statistics 2018, Volume I*, MINISTRY OF HOME AFFAIRS, GOVERNMENT OF INDIA (July 15, 2020, 8:30 PM), https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%201.pdf.

and parcel of our daily life. The data driven society provides easy access to the cyber criminals the information they need and the easiest way to collect the data is from the social media. The popularity of social media platforms is reflected in its user base of 2.22 billion in 2019, which is expected to reach 3.02 billion in 2021. Therefore, the cyber criminals target the social media platform for committing the crimes. To beat the cybercrimes, it is necessary to amend the Information Technology Act 2000 and include new stringent mechanisms to apprehend the cyber criminals. The media which is also known as the fourth pillar of democracy need to work more carefully and prudently so as to play a vital role in making people more conscious and aware while using internet and social media so that, they would not fall prey to the web of cybercrime.

*****

 [ISSN 2581-5369]