# TRADITIONAL JUDICIAL SYSTEMS NEED AMMUNITION FOR FUTURE

**Banipriya Mishra, KIIT University**
**Shreya Chatterjee, KIIT University**
**Supriya Mishra, KIIT University**

## ABSTRACT

*Y2K revolutionized, restructured and reorganized the Indian way of living with the introduction of computers, internet and networking (computer networks). Today computer and smaller versions of desktop computers like laptops, tablets, Ipads and smart phones are a necessity instead of indulgence. Spending more than 60% of waking hours in the digital world, humans today are more accustomed to the cyber world than the real-world. Thus internet is the preferred medium of communication, information and transactions. Having explored the internet some crooked minds inclined towards crime tends to use the internet and its associated paraphernalia for commission of unlawful act owing to the anonymity, obscurity and inscrutability internet provides.*

*The existing legal framework does not have enough teeth to deal with crimes conducted using digital devices and digital networks. The culprit can easily plan, execute and effectuate a crime without actual presence at the site of crime, thus making it complicated, confusing and confounding for investigators, law enforcement officials and traditional justice systems which are completely dependent on physical evidence to identify the real culprit or to ascertain guilt and decide the amount of punishment. Using a desktop, a laptop or even a smart phone, the criminal can harness the power of internet, Wi-Fi technology, Bluetooth, 4G data speeds and proxy-servers to execute an illegal offence even when he is miles, countries or continents away from the actual location of the crime, thus leaving absolutely no physical trail of the execution of the offence. Considering such possibilities stimulated by technical advancements, it becomes necessary to employ digital footprints as they are the only way to determine the factualness of execution of an unlawful act and to pinpoint the real culprit. Digital footprints have to be given their rightful place in the existing legal framework to facilitate verification of execution of an unlawful act, spotting the actual culprit and determining the amount of punishment.*

*This paper is a detailed analysis of existing legality and legal framework to enable understanding, recognition and acceptance of the significance of digital footprints for both traditional and New-Age crimes and utilization of the same by the current Justice Systems to corroborate, attest and substantiate the execution of an unlawful act.*

**Keywords:** Digital, Footprints, Technology-Aided Crime, Justice, Crime, Real, Culprit, Internet, Current Laws.

## INTRODUCTION

The cutting edge brought about in the Indian society with the opening up of Videsh Sanchar Nigam Limited (VSNL) to the public platform on 15th August, 1995 gradually revolutionizing the virtual world from the cult of using dial-up modem connection services giving way to the easily available 4G services today and 5G just on the verge of being introduced in the market has resulted in doubling of broadband internet users to about 563 million in March 2019 It has accounted India to score well on the grounds of availability of internet on the basis of its affordability , mobility and applicability aspects. India now ranks at 47th out of 100 countries globally on inclusion of internet India avails the world's cheapest mobile data at USD 0.25 per GB and with reduced prices in mobile phones, data plans and various modes of digital payment options it is slowly gripping up and has penetrated well within the lower socio economic classes and rural towns and informal settlements. Today, India has made its stand amongst the top three countries in the world, second only to China in digital consumption of services

Internet messaging applications like WhatsApp and Face book have become the biggest drivers of internet in India helping people in maintaining their connectivity with each other, providing them with a platform to have accessibility to different kinds of share worthy content. The overt reliance of people on internet for carving out a niche for themselves through the use of various online applications available is making millions of people here vulnerable to new forms of crimes being committed online or age old crimes being committed by perpetrating latest techniques in the virtual world. It has been reported that at least one crime is committed using digital devices in every 10 minutes in India.

There has been a substantial change in the understanding about the way in which a criminal mind is operating and also the reasons behind a myriad of deviate human behaviour. In India, the law enactments and judicial approach in connection with the crimes committed by using digital devices is not in pace with the current technological development, though punishments attached to it are not meagre but there are loop holes which is helps an individual from avoiding sanctions. Thus, for formulation of proper legal framework which can combat with the e-crimes committed today there is a need to adapt with the latest digital technology and complying with it. Crimes like face book hacking, email spoofing, online money laundering are taking a toll in India with very less conviction rate. The fear of getting entangled with legal proceedings for unavailability of proper procedural legalizations along with the disappointment about the quality of service being provided, the Internet users do not prefer to file their cases with the police which are leading to less than 50% of cases being registered with the police department. A recent study conducted has revealed that India is ranked amongst the top 10 countries in the world as being one of the most vulnerable country to online crimes According to a report, there are around 5000 complaints been made with the police department regarding online crimes out of which arrests regarding 2000 has been done of which around 12 are merely convicted.

India has responded very lately in providing internet infrastructure and only in the year 1998 the Indian Government established National Information Technology task force with an objective to suggest ways and means in facilitating e-commerce (Ahmad, 2011). But within a short span of time it is quite notable that India has tried to adapt with the changing technological trends and has recently included some extremely important amendments in law. Yet there are

essential legislations required with effective sanctions to cater to the growing demands of technology providing the implementing authorities with proper training and power in making them enforceable adequately. The Law in India helped the government in forbidding and blocking of websites considering it a criminal offense where messages are being exchanged against the government which is deemed as offensive in nature. More than 20 people have been detained by officials in 2018 for making derogatory online comments in various social media platforms including WhatsApp involving religious and political matters ranging from the Central governments demonetization policy, regarding elections and posting of abusive comments against political leaders, to messages hurting religious feelings of people including water row between the states of Karnataka and Tamil Nadu.

The Government owned Central Monitoring System (CMS) installed by the Centre for Development of Telematics has given permission to various government concerns and departments for keeping surveillance over electronic communication exchanges made in real time without giving any information to the person whose messages are being tracked who may be a common citizen or a person holding high pedestal. It is a centre, which allows developmental works concerning telecommunication technology to commence smoothly and its data-mining programs giving the various security agencies, income tax officials access to the centralized telecommunication network providing them with the permissions for listening and recording of electronic communications of individuals made over landlines, mobile phones, satellite phone calls, and Voice over Internet Protocol enabling them to read private text messages, emails exchanged between individuals, monitoring their posts shared on social media and tracking their geographical locations in real time, even can search histories on search engines without any intervention from legal or executive body of the government. This surveillance facility has been availed to nine security agencies wings which includes the Ministry of Home Affairs, Intelligence Bureau and the Research and Analysis Wing but the law governing interception and surveillance includes an oversight mechanism to avoid unauthorized interceptions the punishment for which includes fine with maximum prison of three years .These data and information as "*digital footprints*" intercepted is of great importance for being used during prosecution to keep up the "*Digitalization*" of India to enhance but for keeping up with the digital securitization of the country intact there has to be made stringent laws to meet the existing gaps. We thus require more technically sound legislation with proper sanctions and a technically trained efficient enforcement framework to deal with the miscreants effectively (Pandey & Saurabh, 2007).

## Existing Regulatory Scenario in India

The current manifesto of "*Digital India*", leading to digitisation has led to dependency of courts on relying upon computer and electronic forms of evidences during prosecution of crimes committed using digital devices which is still in the nascent stage. In general the Indian government is trying to adhere with the fast paced technological developments by following the process of adjusting with the current scenario by following three major steps of making adjustment with the already prevalent National Laws, identification of gaps in the existing legislations and drafting of new legislation to comply with the existing legal loopholes.

Today, crimes are being committed by intelligent highly skilled technical professionals to which the skill and acumen of investigating officers remains unrivalled. There is requirement of

hyper technical squad with sharp acumen to deal with crimes committed using digital devices. With the marching of our economy towards complete digitalization process at a break neck speed along with the increasing ability for collection, along with usability, analysis of huge amount of digital data about every nuances of life with the trail of browsed machine readable information left behind because of increased usage of individuals for their every personal, social, official and business communications commencing over the digital platforms.

The Supreme Court has now allowed acceptance of evidences in electronic format without a Certificate under Section 65B of Indian Evidence Act, 1872 but it has to be the "best evidence" and a primary form of evidence which can provide enough support in proving or disapproving a fact in a case. It has to adhere with maintaining the integrity of the format without tampering of it, has to be in accessible condition for reproducing it in the court of law in its original form and for adequate acumen in identifying legally supporting viable proofs which have no effective legislation till now and requires adequate amendments to meet the enhancing technological misuses being made by the criminals.

The Information Technology Act, 2000 also known as Internet Law or Indian Cyber Act has paved the way for recognition and has brought all the records in electronic format , all online transaction communicated and all the data and information trails left behind during browsing of internet under the purview of Law. Section-4 of Information Technology Act, 2000 has given recognition to acceptance of electronic record and has made it acceptable as legally valid generally. The primary objective of framing the Act was to curb misuse of computers for committing crimes, for stopping of falsification of data and information and transactions performed in the digital platform. The Information Technology Act, 2002 only revolved around the crimes committed in the intangible cyberspace and the business transactions accomplished through electronic mode in India. Though the above legislation only laid down a foundation structure for working through networked communication smoothly but the most formidable amendment was made in The Information Technology (Amendment) Act, 2008 which dealt with the legal challenges connected with the world of "*internet*" and remarkable amendments were made which laid down the edifice for building up of formidable legislations pertaining to security and even amended some terms including the definition of "*communicating devices*". Then after in accordance to the uprising needs of the society, legislations were minimally changed to meet the criteria for adhering with the political situational requirements which were caused due to networked communication discrepancies without making any permanent resolution to it (Walden, 2016).

The Supreme Court in the year 2015 had revoked certain provisions related to the Information Technology law and has provided restriction on the contents being published on the digital social medium platform keeping intact the authority of the government for issuing orders for blocking the contents online "*in the interest of sovereignty and integrity of India, security of the State, and friendly relations with foreign states or public order*" without requirement of any approval of court. The Ministry of Communications in the year 2017 allowed for disrupting telephone, mobile and internet services temporarily during a "*public emergency*" or for "*public safety*". An amendment in Information Technology Act was done through the Finance Bill merging the Cyber Appellate Tribunal with the Telecom Disputes Settlements and Appellate Tribunal in 2017 was done to catch up with the rising trends in the crimes committed using digital devices and provide people with an effective public grievance redressal system (Sharma, 2011).

In 2018 an insightful decision was made due to mob violence which led to 31 deaths which was caused from some messages exchanged over social media platform and Section-79 pertaining to intermediary liability and their protection with regard to unlawful third-party content that may be posted on the websites. Thus, amendment regarding disclosure of sensitive information by body corporate to the third party without obtaining prior consent from the provider of information for identity verification, or for prevention, detection, investigation purposes which included incidents connected with crimes committed on a digital platform for equitable prosecution and punishment of offences which will be disclosed to them by order given to them under law for the time being in force.

In 2019, The National Investigation (Amendment) Bill, 2019 included a bill regarding cyber terrorism committed by individuals using networked devices under Section 66F of Chapter XI of the Information Technology Act, 2000 (21 of 2000) It has been included in the list of scheduled offences committed under section 2(1)(f)and has allowed under Section 1(2)(d) for checking of these kind of offences committed across borders of India which have been designed against the citizens of India or affecting the National interest of India as a whole which gave them an upper hand in dealing with the labelled terrorist as prior legal regime made it difficult for them for carrying out investigation process

The recognition of future possible crimes committed by the usage of digital devices with inclusion of latest technological processes or devices which are taking a toll of the government requiring them for making amendments which are necessary for the formulation of contemporary laws. The current legal regimes of India is posing a major threat for the investigators and the law courts which are not adequately framed with meeting the current crimes committed through electronic medium to be effectively and efficiently dealt with. In India the enactment of Information Technology Act, 2000 and consequential legal amendments made in the Indian Evidence Act, 1872, the Indian Penal Code, 1860, Criminal Procedural Law, 1973, the Reserve Bank of India Act 1934, Banker's Book Evidence Act, 1891 , Negotiable Instruments Act, 1881 allows for making of evidences in the digital form to be recognised and made acceptable in the court of law for booking of masked criminals behind the networked community to be brought to the forefront and punished equitably but still there is a lacuna revolving around the data sharing and jurisdictional issues, different perceptions in acceptance of a legislations amongst different places , and the problems revolving around enforceability.

In the case of Anvar P.V. Vs P.K Basheer and Others, (2014) 10 SCC 473 had spoken about the genuineness of the electronic record produced during prosecution and had held that the computer output has to adhere with the conditions specified in Section 65B (4) and comply to it equitably for making the electronic record admissible in the court of law. It had overruled the judgment laid down under State (NCT of Delhi) Vs Navjot Sandhu alias Afsal Guru (2005)11SCC 600 by two judge bench of Supreme Court had observed "*to the extent that admissibility of electronic evidence pertaining to electronic record of this court, does not lay down correct position and is required to be overruled*" which had brought to rest various controversies arising out of acceptance of electronic evidences in the court of law providing a form of guideline regarding it being practiced at various High Courts and the Trial Courts in India.

In the case of Suvarna Musale Vs Rahul Musale 2015(2) Mh.L.J. 801 it has been held under Section 65A and Section 65B of the Evidence Act, 1872 that recording made by taking the help of electronic and digital technology or mechanisms for producing the same during

prosecution as electronic form of evidence has been given due weight age, acknowledgement and recognition in today's legal framework as it revolved around a genuine problem of a wife who was the petitioner in the case having a minor child of about 6 years living and working abroad in U.S. and for being physically present in court of law for her prosecution was expensive and she had big complexity in getting leaves from her job for it along with the VISA processed thus allowing her for video conferencing. Section 4 of the Information Technology Act, 2000 provides that the data and the information has to be in written electronic format which can be directly accessed for references subsequently.

But a division bench has given a judgment in Shafhi Mohammad Vs State of Himachal Pradesh (2018) 2 SCC 801 where they had "*clarified*" or made it clear that under Section 64B(4) it was required for a certificate to be produced in court of law for acceptance of the electronic record as evidence for clarification in a case which was just imbibed to follow procedures and could be relaxed by Court when there is a need for equitable justice to be imparted like a particular digital device may not be in possession of a party during the prosecution of a case and as a result it will be unwilling on the part of them in securing the requisite certificate required for adjudication of matters pertaining to the case thus, considering it unnecessary.

In Arjun Panditrao Khotkar Vs Kailash Kushanrao Gorantyal ,(2020) SCC Online SC 571 itwas decided on 14.07.2020, in which the Supreme Court has "*clarified*" about acceptance of electronic records as evidences during adjudications without producing requisite certificate in accordance to the provisions laid down under Section 65B of the Evidence Act, 1872. It comprised of a three judge bench which has held the judgment made in Shafhi Mohammad Vs State of Himachal Pradesh (2018) 2 SCC 801 as completely incorrect pertaining to securing of requisite certificate under the section where a party connected in an adjudication is not in possession of the electronic or digital device which is required to be produced an evidence in court. It has provided for writing an application to a judge for production of the requisite certificate needed in adjudication of the case where the person who is in actual possession of the device in question does not agree to provide it to the concerned party under Section 65B(4) of the Evidence Act ,1872.This case has also clarified the confusion over a sentence mentioned in Anvar P.V. Vs P.K Basheer and Others, (2014) 10 SCC 473 where the last sentence of the case had mentioned that in case if an electronic record which has been produced in an adjudication as a primary form of evidence under Section 62 of the Evidence Act, 1872 it can be accepted as an electronic evidence and does not require complying with the provisions and condition precedent made in Section 65 B of the Evidence Act,1872. It has "*clarified*" that if an electronic evidence is produced in its original format during an ongoing adjudication of a case which provided that the owner of a digital device can step into the witness box and giving his testimony as him being the sole owner or sole operator of the concerned device in question or in case where a "*computer*" turns out to be a part of a computer system or network and the party in question provides his complete unwillingness in producing the requisite data and information contained in such digital devices in the form of electronic data then it can adhere to Section 65B(1) along with the required requisite certificate mentioned under Section 65B(4) of the Evidence Act, 1872 to comply with it.

In case during a trial, a party is unable to produce an electronic record due to false certification given or demanded certificate was not handed over to him by the concerned person the requisite judge conducting the trial can summon the person/s as referred to in Section 65B(4) of the Evidence Act, 1872 and require that such certificate, be handed over to the party by the

person concerned in case circumstances emerge concerning production of electronic evidences and no requisite certificate pertaining to it was made but it is subject to discretion exercised in civil cases and is done in accordance to the requirement of facts in cases for impartment of equitable justice. But in case of criminal trials there is general principle providing for the accused compulsorily being supplied with all documents which a concerned prosecution is seeking in relying upon before the initiation of the trial under the provisions provided under relevant sections of Criminal Procedural Code.

General Directions have been issued by the bench in this case with relation to the cellular companies and the internet service providers for maintaining of CDRs and other electronic records of relevancy to the case for the period said (in accordance with Section 39 of the Evidence Act, 1872) concerning which the records had been seized when the investigation was carried out regarding it and is required to be securely and separately maintained. When the parties involved in the case in question would need the electronic records for proving their defences or in case of cross questioning any witness of the case these can easily be summoned upon .It will also be applied to criminal trials for ensuring that they are preserved well and can provide certificate required to be issued as and when required during different stages of the continuing trial process. These provisions are to be followed till the data retention provisions are framed for the telecom and internet service providers to abide by it.

The Court in the above case has requested and directed the government to frame legislation and provide for provisions and directions under Section 67C of Information Technology Act, 2000 for inclusion of rules in retaining of electronic record collected during an investigation of a case, segregating, framing laws for maintaining the details about chain of custody of the electronic evidence in question with proper stamping and maintenance of record and storing of it to be produced in court as required at different stages of the ongoing trial process or appeals in Court. To also formulate unbiased legislation for preservation of data and information for curbing the corruption practices involved in changing the electronic documentary evidences. It has also brought into purview that there is a need to frame appropriate legislation for proper preservation, for retrieving the electronic data and information accurately and reproducing of the same in the Court as indicated for consideration in a Committee Report constituted by the Chief Justice's Conference held in April, 2016 and adhere to it for framing necessary changes required.

Section 61 to 65 of Indian Evidence Act does not contain provision to accept "*electronic documents or contents of electronic documents"* which had been done with exclusive intention of the legal framers not to override Section 65B and it had been included solely to meet the growing technological scorn reproducing the technical evidences during the judicial proceedings as proof in suffix of a crime. Section 65 B of the Evidence Act allows secondary form of evidences comprising of computer print outs or data copied on electronic /magnetic media to be accepted in the court of law as the data and information stored in computer are in machine language are available in large sizes which requires an interpreter to decipher them.

Thus, regulations regarding Digital footprints, being directly accepted in prosecution are still in a nascent stage, the legislation does not provide formidable regulations of easily accepting or a direct approach of acceptance towards such proofs and evidences, with the exception of some cases which are trivial not of utmost importance or setting an example for the society at large. The Courts are reluctant to completely rely on such evidences as there are still no flawless and formidable regulations formed, which will bind the offences within the legal framework

completely for them being volatile and tamper able in nature. Jurisdictional issues also pose as major hindrance for a case being resolved. There are lacuna in legislation regarding collection and preservation as storing of such information is very difficult sometimes, the experts are not adequately trained or it is very difficult for them to keep up with the changing technologies for the crimes committed by using of digital devices are usually committed by white collar technically skilled people even the law enforcement officers, legal fraternity and the juridical framework are not equitably trained and don't understand the fast paced technologies to adapt with the changing scenario (Kamath, 2014).

## Notable Trends in Indian Crime Scenario

There has been a major paradigm shift in the way communications are being exchanged between individuals. Nowadays both official and unofficial exchange of data and information is being commenced through the digital platform. Emails and Social media platforms are immensely being used for exchanging communications online. Official meetings, exchange of important official documents, exchanging of details regarding meetings of utmost importance, emergency business meetings, major business dealings and papers adhering to it, unofficial meetings, exchanging of unofficial communication are all being performed at the digital platform by emails, social media websites ,online business websites, online official websites, instant messaging apps which is leading to saving of time spent on commuting from one place to another as internet is not bounded by boundaries and is cost saving in nature .It has become important to save the messages, conversations exchanged and documents for any mishap relating to misuse of the digital platform for supporting their cases in the form of electronic record which could be produced in court of law but as certified primary evidence or secondary in nature.

Instant messaging app WhatsApp has gained an edge over the other instant messaging app with over 1.5billion active users. It has been quite notable that as an instant messaging portal WhatsApp has been considered as playing a key role in spreading of fake news through the usage of its "*Forward*" tag which was newly introduced in it in 2018 which led to killing of 20 people because the message led to causing of mob violence about religious and communal issues leading the company in updating its Frequently Asked Questions (FAQ).

The company had decided to take legal actions against users for activities such as "*bulk or automated messaging*" and has also taken steps and making diligent efforts in identifying the accounts misutilising the messaging application which has led it to banning of two million accounts all around the globe in a month

The advancement of technology and massive use of internet had led to a radical shift in its ability of reproducing, distributing, controlling and publishing of data and information which has changed the economics of distribution as increase in speed of transmitting messages about a billion character instantly in minutes cost effectively has made it easier for distribution of unauthorized immoral copies of individuals globally for earning purposes of right holders of original copy or if put up for any vengeance purposes.

The growth of Internet fraud is now almost proportional to the growing electronic business activities commenced through the usage of internet. The new found digital mode of online business activities are being misused greatly by corrupt traders bringing into light a new found class of white-collar criminals.

There has been quiet notable increase in usage of electronic mails as it has been the most convenient, effective and a very popular mode of exchange of communication amongst individuals both for official and unofficial purposes which are being used unscrupulously in commission of heinous crimes like perpetuating frauds, for the purposes of commencing scams, in carrying out terrorism activities and some other immoral activities.

The increase in usage of social media platforms has widened the reach of stalkers globally as they can easily impersonate the victim for harassing and humiliating him without revelation of actual identities for instance a stalker can use various ways of trapping the victim by showering the receiver with letter of praises and love letters. When the sender feels the receiver is slipping away from his trap or is not responding to him the he may become aggressive by sending aggressive and threatening or intimidating emails with file attachment of obscene materials even to the extent of using live chats and Inter Relay Chat for being in direct connect with the victim in question and carrying out various ways of victimizing the individual with dire consequences if the latter severs the ties with the stalker and in case of non responding him.

Internet is multifunctional in nature (David, 2019). In India there has been a rise in "*denial of service*" activities which takes place when there is some form of disruption in transmission of data and information over the internet takes place as the complete transfer involves a "*three way handshake*" in which when information is placed with another computer it is known as client computer and with which request is made to is called server computer.

The multifunctional nature of Internet has made mockery of the effective functioning of India's current regime. Though India is trying to cope up with the constant new technically effective society efficiently there is a need for rethinking and reorientation of the current legal framework to accommodate the latest developments in digitally committed crimes within its purview.

According to a report titled, "Internet in India 2019" by Nielsen with Internet and Mobile Association of India (IAMAI) has revealed in a study which has taken into account that per head counting of citizens of India having accessibility to internet are using it for their official and unofficial communications have noted that till 31st March, 2019 there had been a total of 451 million internet users monthly using it actively with a continuous rising streak of which 385 million internet users are coming under the age category of 12 years and above while 66 million users are between the age bracket of 6 to 11 years accessing internet with the devices of their family members. Though there has been an imbalance of population distribution amongst the urban and the far flung areas still internet has set its foothold on a higher note in the urban areas with 72% of the total base internet users resulting into a total head count of 139 million internet users in day to day life. Even though the total internet base users total head count has accounted for 192 million users in the urban areas still there has been an even split amongst the urban and rural internet users where the female internet users have accounted for around 149 million compared to a total of about 258 male internet users (Bhumika, 2019).

According to the "*Norton Life Lock Cyber Safety Insight Reports*" which was conducted online by the Harris Poll on behalf of Norton Life Lock had taken place amongst 10,063 adults from 10 countries reporting that criminals through the usage of networked connectivity have been successful in swaying away 1.24 trillion rupees from Indians only during 2019. While 80 % of the total Indian respondents have been victimized under the digital surge till date with 66% from it having faced only in 2019. 63% of Indians have been hit financially. The study has surfaced that amongst 10 consumers of internet 4 have fallen victim to identity theft that is 39 %

of the total Indian respondents with 10% having faced only in the year 2019. Though while 63% of the respondents are still ignorant about the way they will act in case of happening of identity theft with them 70% are sure about their online identity being stolen in near future (Riju, 2019).

The Central Monitoring System (CMS) developed by The Centre for Development of Telematics which is owned solely by The Government of India for development of telecommunication technology has a centrally installed data mining program for the purpose of monitoring of a subject in real time allowing for intercepting, decrypting and blocking of websites or any form of communications made over the internet providing for complete electronic surveillance over them. Both the Central and the State government has been provided with permission to issue directions against any form of misuse or immoral or illegal usage if has been done by any subject in any form by using internet. The law has even provided for punishment in case of unauthorized interception which includes a maximum prison sentence for three years or fine or both. This surveillance facility has been majorly made available to nine government security agencies for monitoring of information causing hindrance to the country or if in some way posing harmful to the common masses at large.

According to Ritesh Chopra, Country Director, NortonLifeLock, India, though there has been an upsurge in online committed crimes of identity theft, data theft and online fraud in India consumers here even if are concerned about their personal sensitive data being misused still are very comfortable in sharing their data and information with the third parties if they receive something in return for it. He has said that it is very crucial for every individual of us of being mindful about our digital footprints being created about the form of data and information being shared actively by us with the third parties and the degree of accessibility we are providing them through devices used by us.

According to a written reply made by Union Minister of State for Home Affairs, Shri G Kishan Reddy to a question brought about in Lok Sabha has said that there has been a continuous rise in people being victimized under online frauds. As per data of National Crime Records Bureau has started collecting data separately for online banking frauds starting only from the year 2017. 3466 online frauds were recorded in the year 2017 and 3353 cases in 2018 respectively. India has recorded cases of online crimes committed in the year 2014, 2015, and 2016 as 9,622, 11,592 and 12,317 respectively.

According to a Webinar which was hosted by the United Nations Women in collaboration with the India Future Foundation on the topic "*Cyber Crime Trend and Digital Safety amidst COVID-19 Pandemic*" which has concentrated majorly on the promotion of safer, better and equitable digital platform and sensitivity towards responses made towards women online. According to the United Special Reporter, women are majorly becoming a soft target online which is resulting in harming them psychologically, physically, sexually and economically. It has reported that in between the months of March and April 2020 India has witnessed an astounding 86% rise in cyber-attacks.

In the case of Subhendu Nath V State of West Bengal, 2019 SCC Online Cal 242 order dated 18th February, 2019 A division bench which comprised of Justice Manojit Mandal and Joymalya Bagchi, JJ in the Calcutta High Court has given directions for ensuring proper, equitable and effective investigation of crimes which involved any form of electronic record for keeping up with the rising trend in mishaps caused through the usage of internet and has further said about the requirement of proper training of police officials for equitably collecting,

receiving, storing, analysing and reproducing the electronic records as digital evidence in the court of law in a formidable manner (Devika, 2019).

According to the Facebook's Transperency report, Indian government has made data requests of accounts involving 22,024 data made in 2017 which is 61.7 percent rise from 2016. It has even revealed that Google has received about 14,932 user data disclosure reports from the government and Twitter had received 576 account information requests made to it during the same time period. In July, 2017 Government of India had announced for blocking of 1,662 defamatory websites on the social media platforms on the request of law enforcement agencies blocking 956 sites in Facebook, 409 on Twitter and 152 on YouTube amongst other, the number of URL blocked were double in comparison with previous years.

Electronic records are usually being considered in the Court of Law as Secondary form of evidences as they can easily be tampered. Though the electronic records are being considered to be reproduced in the Court of law as evidences still they require strict rules to adhere to as any deviation leads to it being rejected. Today, digital modes of evidences are being used during judicial proceedings but they are open to all kind of susceptibilities. According to Section 92 of the Information Technology Act, 2000 the Indian Evidence Act has been amended under Section 3 for providing permission to all form of electronic records for being produced in Court of Law to be used during investigation purposes. Section 59 of Evidence Act uses the words "*contents of document or electronic records*" and the legal framework has allowed for insertion of Section 65A and 65B for allowing admission of electronic form of records as evidences The Courts have allowed for inclusion of electronic records as electronic evidences to be reproduced during judicial proceedings if they adhere to the requisites contained under section 65B of Indian Evidence Act, 1872. Still there are unresolved vent about which the legal framework is still quite about is if a secondary form of electronic record is seized from the accused itself for reproducing in the court of law as evidence and no support under Section 65B could be taken then the accused cannot be compelled to stand as a witness against self as per Article 20(3) of the Constitution of India.

## Precedance of National Security Design for Data Security over Data Privacy and Human Rights

Countries are still in a crux in the international arena about whether they should make better regulations and keep intact the data security regulations for prevention of crimes committed using the networked connectivity or whether they should support the data rights in context of human rights which is the main cause of contention for digital footprints being enacted equitably as the time demands. There is a growing need for developing specific legislation for dealing with digital footprints which requires strong collaboration amongst countries for proper sharing of expertise, data and information amongst countries in dealing with online crimes in a regulated manner within time assigned.

Data Securitization is a technical issue which revolves around curbing the access of unauthorized entities by individuals with the aim for providing complete protection and securitization of personalized data and information exchanged or stored or interacted or used in the digital platform. While Data Privacy is a legal issue about providing authorized accessibility to entities by individuals for using or for not using their personal sensitive data and information.

Though data security and data protection of Indians are of equal importance for the current government they are trying to form proper legislation pertaining to them. While designing of National Security Design for data actively requires to be cocooned by proper legislation for helping companies, organizations and individuals from getting attacked by using of the networked connectivity. Designing of Data Privacy Laws is of equal importance for retaining of human rights of people as it would provide stringent laws for drawing a limit on prioritizing a consumers approval for using or for not using of his personal sensitive data and information by the companies, organizations or corporate before accessing and processing the same.

The protection of data and information holds priority over ensuring privacy of them as if personal data gets caught up with the risk in any form of security breach which cannot be curtailed then privacy of an individual cannot be assured to him. Thus, it can be said that though personal sensitive data and information can be protected but it cannot be held completely private in nature revealing that data protection revolves around technology while data privacy is pertaining to the legal arena.

As India is marching ahead steadily towards accomplishing the aim of the current government in converting their dream of Digital India into a reality it has led to increase in its associated risk arising due to internet becoming indispensible to its citizen at large. It has considered in instilling data and information security for becoming a major part of our redesigning of national security. Thus, there are more adherences towards creation of strong data security architecture with proper legislation to be abided with in view of helping the government to monitor and to strengthen the networked connectivity within India intact.

With criminals using latest technologies both in commission of old and newly designed crimes through the usage of networked community India has become more susceptible to crimes like identity thefts, stealing of data and information of National importance or with high commercial value, online frauds, disruption of services like attacking open servers, digital assaults , the increased outsourcing partners in business houses are posing great hindrance for data sharing with is no longer curtailed with the insiders of the company for which even small working mistakes or any mischief on part of an employee is leading to long term losses and creating a negative reputation of the concerned company, terrorism activities being carried out online with latest modes, techniques and processes with malware attacks like Advanced Persistent Threats(APT) and Distributed Denial of Services (DDoS) According to a study "*Cost of Data Breach Study in India 2016*" reveals that the average total cost per data breach paid by an Indian Company has risen by 9.5%.

The current technological advancements has led to the enactment of the Information Technology Act, 2000 and has even led to the amendment of Indian Evidence Act, 1872 in the year 2016 for recognizing and using of electronic record for reproduction of the same to be made during judicial proceedings as evidence in dealing effectively with crimes committed through the usage of digital devices. But due to major issues in providing for evidences to be produced in court of law as primary or original it has otherwise been accepted as secondary form of evidence just for providing support to the actual evidences given and are considered to be circumstantial in nature and can easily be tampered, changed, altered with thus, allowing for production of such form of evidences with a certification under Section 65 B of Indian Evidence Act, 1872 providing for it to be correct. For instance there are requirement of transactional histories, proofs of relationships currently amongst people, mobile phone call histories records which involves

opposite parties providing supplementary proof for dealing effectively with any form of electronic record. But sometimes chats or message exchanged between individuals cannot be produced as the companies' servers are located in foreign lands and permissions are required for getting the end to end encrypted messages to be deciphered. Thus for reproduction of electronic record during judicial proceedings, some companies having a policy of privacy are denying for providing lead to the law enforcements on the grounds of privacy laws which is helping criminals in hampering the security of the nation at large (Manoharan, 2020).

According to an officer of Data Security Council of India (DSCI), established by NASSCOM for promoting data protection on the condition of anonymity has revealed that India lacks extensive, elaborate, clearly outlined models revolving around data and information to be shared with the investigating agencies which is keeping their finger crossed while facing technologically emerging new threats. He has further said that there is no requisite standard procedures adopted by Indian administration which have been documented for seizing of electronic records in the form of digital footprints to be presented during judicial proceeding as digital evidence (Arunabh, 2016).

For instance the Indian Government is very much worried about social media platforms like Whats App and Face book are being allowing for creation of grounds for passing of fake videos for panicking people or misguiding people and are even being used by terrorists for spreading of data and information easily encrypted through various modes of cryptic messages, video songs, paedophilia rings. Though Whats App is reluctant in allowing law enforcement officers in tracking of users as its services follow the end to end encrypted services but they have been made to consider the vulnerability, misuse and manipulation of data and information exchanged while making the Government to allow citizens in filing of cases with cyber police on commission of unauthorized intrusion if an users feels has been victimised under it.

## CONCLUSION

The existing legal regime is still in a nascent stage with The Information Technology Act, 2000 which had been brought into legislation enthusiastically for adopting the Model Law brought about by The General assembly of the United Nations for keeping in with the recommendation of International Trade Law dealing only with reduction of paper evidences being made in Courts. The Information Technology Act, 2000 has been continuously amended along with Amendments being made in other Acts acting as fillers for keeping a check over the growing traditional and new form of crimes being committed using the digital platform and catering to meet the demands of continuous technological trends trying to curb them. It has now reached completely new heights for which it requires better, proper, comprehensive and well defined legislation which has been discussed in length in this chapter regarding upper hand of securitization laws over privacy laws for providing people with a secured digital platform to exchange both personal and professional information unaffected. It has been observed that specific legislation is yet to be developed to deal with digital footprints and there is a requirement of collaboration of opportunities to share output in cases and investigation amongst various investigating agencies in India for exchange of expertise and sharing of data and information for dealing with crimes committed by digital devices in appropriate manner and within a designated time frame.

## REFERENCES

Ahmad, F. (2011). Potential and Problems. *Cyber law in India (law on internet).*

Arunabh, S. (2016). *Why most cybercrimes in India don't end in conviction*. Retrieved from https://www.linklaters.com/en/insights/data-protected/data-protected---india

Bhumika, K. (2019). *Internet in India 2019: Equal split of internet users in rural and urban areas*. retrieved from https://inc42.com/buzz/internet-in-india-2019-equal-split-of-internet-users-in-rural-and-urban-areas/

David, A.A. (2019). *Cybersquatting and online trade mark/cyber mark protection*.

Devika. (2019). *Case briefs of high courts.* Retrieved from https://www.scconline.com/blog/post/tag/cyber-crimes/

Kamath, N. (2014). *Law relating to computers, internet & e-commerce: A guide to cyber laws and the information technology act, 2000 with rules, regulations and notifications.* India: Universal Law Publishing Company Pvt. Limited.

Manoharan, G. (2020). *Partner, JSA, security columns news, by express computer*. Retrieved from https://www.expresscomputer.in/security/admissibility-of-electronic-records-as-evidence-in-india/53777/

Pandey, U. S., & Saurabh, S. (2007). *E-commerce and mobile commerce technologies*. S. Chand Publishing.

Riju, M. (2019). *Economic time's bureau, cyber criminals stole Rs 1.2 trillion from Indians in Survey.*

Sharma, V. (2011). *Information technology law and practice.* India: Universal Law Publishing.

Walden, I. (2016). *Computer crimes and digital investigations.* United Kingdom: Oxford University Press.