

DOI: 10.5281/zenodo.121126188

# AN EMPIRICAL STUDY ON USAGE OF DIGITAL FOOTPRINTS AS EVIDENCES DURING LEGAL PROCEEDING A STUDY BASED IN ODISHA

Banipriya Mishra<sup>1</sup> and Supriya Mishra<sup>2</sup>

<sup>1</sup>Assistant Professor I, KIIT School of Law, KIIT Deemed to be University, [banipriya.mishra@kls.ac.in](mailto:banipriya.mishra@kls.ac.in)

<sup>2</sup>Lecturer IT, Skill Development & Technical Education Department, Government of Odisha, [supriyamishra8@gmail.com](mailto:supriyamishra8@gmail.com)

Received: 20/10/2025  
Accepted: 24/01/2026

Corresponding Author: Banipriya Mishra  
([banipriya.mishra@kls.ac.in](mailto:banipriya.mishra@kls.ac.in))

## ABSTRACT

*The current upsurge in the digital infrastructure of India has given a solid foundation for using the digital traces left behind as a trail of data and information in the form of digital footprints, whether they be structured or unstructured, related to time series, or specifically related to any happening of an event that is recorded in the form of system or linked data. With the advent of technology and the use of high-end tools, the face of commission of a crime has changed with time, becoming Technology-Aided Crime, which in turn has led to transition of physical crimes into parallel digital crimes. Digital devices and the newest technological innovations have made it possible for criminals to commit traditional or modern forms of new age crimes without physically being present at the scene, making it very challenging for investigators, law enforcement officials, and other traditionally operating legal systems to identify the real offender, determine the guilty, or determine the degree of guilt. In this Article we have taken a sample study based in Odisha to visualize the lacuna in the legal framework which is posing as a major hindrance in facilitating usage of digital footprints during court proceedings at a micro level. Thus helping us in getting an insight over the problems being faced in its acceptance as evidences leading us to decipher the lacunas in Information Technology Act, 2000.*

---

**KEYWORDS:** Digital, Footprints, Technology, Crime, Evidences, Proceedings.

---

## 1. INTRODUCTION

“Security of the citizens at peace time is very important because State is the only saviour of the men and women who get affected only because of negligence of the State” – Chanakya

### 1.1. Digital Footprints

Digital foot prints are the traces left behind by people when they use the internet be it for any purpose –be it to pay their bills through Paytm, or chat with their friends on messaging websites , post travel stories on Instagram or photos on Pin interest , purchase clothes/footwear/accessories /jewellery from online stores like Flipkart.com or furniture from UrbanLadder.com or daily grocery from Grofers.com, order food on Zomato.com, use Google Maps to navigate their journey through crowded roads of burgeoning cities, book movie tickets at Inox.com, check email, post fan fictions on Indiaforums.com, book a taxi on Ola.com, logging into digital classrooms, watching web series on Alt Balaji, execute online transactions on onlinesbi.com, reading stories on kindle.com.

Justice Sanjay K Kaul <sup>1</sup> said that “something interesting is happening” because the users of networked connectivity have left behind much more meta data trails than humans had ever done before the new technically advanced “World Wide Web” was developed. He has further pinpointed that as we are moving rapidly towards a digital economy and are becoming more dependent on services received through internet we are leaving behind us an increasingly deep and active digital footprint.

Digital footprints are trails of metadata left by anyone using Internet which includes the websites visited, emails sent, apps accessed through Androids, Smart phones, Internet of Things (IoT) and information we provide to obtain online services.

Thus, Digital Footprints can be defined as vestige of data and metadata left behind by an individual while using an electronic gadget consciously or subconsciously, which helps in setting aside of crimes committed having no physical traces leading to capture and custody adding viability in proving an

accused guilty or not guilty.

There are two different types of “Digital Footprints” which can be either solid or volatile in nature they are –A “passive digital footprint”<sup>2</sup> is one left unintentionally while accessing Internet. The server connected with the web logs the IP address while surfing internet and changes with every session of logging into the Internet, it is still considered as digital footprint as it gives an idea about the web server used to access websites.

An “active digital footprint”<sup>3</sup> includes data consciously or knowingly submitted by the user to any website. Sending an email is an example of active digital footprint, since it is known that the data will be seen and/or saved by the recipient. Writing blogs, posting tweets on Twitter, every post made on Messages sent across through Meta and even images and videos shared on online is adding to our digital trail as a form of footprint.

Thus, anyone who accesses the web, cyberspace and Internet creates a digital footprint.

### 1.2. Digital Footprints: Technically the Third Eye to Solve Cyber Crime Issues

The technological evolution has increased the importance involvement and usage of the same in everyday life. The word “E” has suddenly acquired demi-God status cause in today’s times we cannot imagine our lives without e-Shopping, e-Banking, e-Payment, e-Doctor, e-Nutritionist, e-municipal Corporation, e-libraries and e-courts. But the same technology is also being used by anti-social minds for illegal purposes. Crimes related to cyberspace are termed as cybercrimes.

Crime can be described as an action or activity considered to be beyond the acceptable social behavior which is punishable. It is basically a deviation from the norms established as the way to interact and behave in a civilized community.

Law establishment institutions have been empowered to formulate these rules, regulations, constraints and conditions to be followed by each and every element of the society so as to make it conducive to accommodate different view-points, perspectives, choices and beliefs. Any departure,

<sup>1</sup> Anand, Utkarsh. ( August 25, 2017, 11:47 AM IST ), Right to Privacy Case: Supreme Court Says Facebook Knows our Friends, Uber Knows Our Location , “ has discussed in detail about the usage of active and passive digital footprints as proofs for deciding cases which is inferred from Justice Sanjay Kaul inferences” in CNN- News18 <https://www.news18.com/news/india/hscap> [accessed 22 July 2019]

<sup>2</sup> Arakerimath , Prof Anjana R., Gupta Pramod Kumar.(2015) Digital Footprints: Pro,Cons and Future, “has discussed about Passive footprints” in IJLTEMAS volume IV issue X, October ,2015 edition

<https://www.ijltemas.in/DigitalLibrary/Vol.4Issue10/52-56.pdf> [accessed 21April 2020]

<sup>3</sup> Arakerimath , Prof Anjana R., Gupta Pramod Kumar.(2015) Digital Footprints: Pro,Cons and Future, “has discussed about Active footprints” in IJLTEMAS volume IV issue X, October ,2015 edition <https://www.ijltemas.in/DigitalLibrary/Vol.4Issue10/52-56.pdf> [accessed 21April 2020]

variance, deflection, aberration, alteration, discrepancy, inconsistency or anomaly from the above-mentioned rules can be termed as a Crime. Crime can range from simple ones like swindling money to complex ones like impersonation, fraud and forgery to heinous ones like murder, rape and terrorism.

Derived from Latin word evident meaning "obvious", proof refers to the available body of facts, figures, suggestive signs and corollary information that clearly indicate that the statement made or proposition put forward is true or valid. This data can be in the form of eye-witnesses, historical registers, journals, deeds, dossiers, logbooks, diaries, chronicles, catalogues, financial instruments, certificates, and memoirs.

Another very important aspect of proof is it "SHOULD BE ACCEPTABLE" in a Court of law or by any Law-establishment institution. The very essence of evidence lies in the fact that it is the only foundation of verification that the crime was indeed committed (*Van Rooyen, 2004:9*) as well as the yardstick to determine the exact degree of punishment.

Legal proceeding is the formal examination of evidence by a jury or a competent authority in order to determine guilt in case of any civil or criminal aberration by the accused. It is a process in which the appointed judge listens to the statements of eye-witnesses, carefully peruses all related documents placed before the jury, and decides whether the accused is guilty or not and finally determines the quantum of punishment based on the Indian Penal Code, 1860. Crimes today are mostly planned ventures with no physical footprint left behind that can lead to capture and custody.<sup>4</sup> Thus, given that even our smallest requirements are being fulfilled by the internet and web, digital footprints are sure-shot ways of pin-pointing guilt.

- Video footage of the crime by CCTV (originally installed for safety purposes),
- GPS tracking of a mobile phone to determine the location of the accused at the place and time of commission of crimes like kidnapping and rape,
- Interrogation of a witness/accused through video-calls which completely eradicates the issues related to geographical locations of the Court where the hearing is being conducted

and the place where the accused was hiding.

- Audio recording of a crime scene.
- Online bank transactions of the accused before, during and after the crime.
- Biometric data related to entry and exit of the accused from the crime scene at the time of commission of crime and many more.

During the ongoing legal proceedings of Anvar V. P.K.Basheer, <sup>5</sup>The Supreme Court of India realized the significant role of digital footprints to be reproduced as evidences and in a historic judgement delivered on 18<sup>th</sup> September 2014 by the bench consisting of Chief Justice Rajendra M. Lodha, Justice Rohinton Nariman and Justice Kurien Joseph in the Parliament Attacks case and gave an overruling to the previously Supreme Court judgement imparted in the year 1995 in State(NCT of Delhi) v. Navjot Sandhu alias Afsal Guru<sup>6</sup>Justice Joseph imparted a new law with regard to acceptability of digital footprints of online activity of accused and any form of electronic document by the Court of Law hearing a civil or criminal trial as a piece of Evidence with the authorization to corroborate and validate the commitment of a crime along with reinterpreting the applications of Sections 63,65,65B of the Indian Evidence Act,1872.

Are just 50,000 police personnel guard capable enough to protect the law and order scenario in a burgeoning city of almost 2 million and is it possible to always have direct evidence of a crime given the level to which technology has taken over our lives? Electronic data should be considered as the Third Eye ,in today's times of highly planned modus-operandi by criminals as well as limited trained law-enforcement staff in order to validate and ascertain the perpetration of a crime in actuality leading to the accused being proven guilty and worthy of punishment.

With substantive development in science and technology, not only in cases of crime committed in the cyber space but also in traditional crimes the offenders are frequently taking the help of electronic devices. Naturally offenders are leaving digital footprints and many times investigating officers are using those digital footprints either on their own or with the help of the expert to uncover truth. But neither is such digital footprint ever presented to the jury in compliance with the Information Technology Act, 2000 and the Evidence Act, 1872 nor is expected

<sup>4</sup> Rahman, Muthmainur. (February,2019) Senior managing director, head of Middle East forensic technology, in Digital footprints - The key to successful fraud investigations, The Lawyer <https://static2.ftitechnology.com/docs/white-papers/FTI%20Technology%20--%20Digital%20Footprints%20>

%20The%20Key%20to%20Successful%20Fraud%20Investigations. pdf [accessed 3April 2020]

<sup>5</sup> (2014) 10 SCC 473

<sup>6</sup> (2005) 11 SCC 600

recognition given to digital footprints during the trial.

## 2. LITERATURE REVIEW

The internet is becoming one of the fastest medium of life for people for their increase in dependency over technology. People have started communicating more effectively through usage of digital devices rather than physical conversation. (Licklider, 1968)<sup>7</sup> Today e-mail, websites have anytime anywhere technological solutions for the betterment of mankind are offering great benefit to the society at large, giving way to crime commissioned by utilization of these forms of newly developed digital platforms which are posing as major platforms for data and information interchange. "The time for incremental change is long over, the current age is one that requires transformational change that comes only with drastic policy reforms" - 27th July 2016, Shri Narendra Modi, on Government of India on bringing innovation from periphery to center stage and Changing Indian Policy Frameworks. Digital footprint can be defined as "online portfolios of who we are, what we do, and by association, what we know" (Richardson, 2008). It is also known as our digital shadow, the footprints we leave after using internet based devices.

Anita Gurumurthy<sup>8</sup>, has concluded that the digital platform has immensely added to the hindrances of law enforcement agencies posing as increased challenge for the legal enforcement agency which inducing of youth for joining terrorist groups, sharing of defamatory contents, spreading of discord amongst common people within a society and inciting of violence as claimed by The Government of India.

Utkarsh Anand<sup>9</sup> has written in his article that dismissing the attitude, Justice Sanjay K Kaul said that "The digital footprints and extensive data can be analyzed computationally to reveal patterns, trends, and associations

Ex CJI Dipak Misra<sup>10</sup>, in the Indian daily "THE TIMES OF INDIA" has commented that the citizens

of India require to keep a check upon blatantly depending on the digital platforms which would help them in retaining proper cordial relation and harmony within different the societal arenas. He has included in it that the messages circulating on the digital platform are to be blamed for the recent upsurge in cases connected with mob lynching in India.

## 3. RESEARCH OBJECTIVES

- To analyze the concept of digital footprints and to give an insight for designing of relevant laws for future.
- To analyze the concept of digital footprints with special reference to Information Technology Act, 2000.

## 4. RESEARCH QUESTIONS

This study has been designed to resolve that whether a digital footprint is adding to the credibility of legal proceedings?

## 5. HYPOTHESIS

Hypothesis (H) - Information Technology Act, 2000 is inadequate to deal with the emerging issues raised by Digital Footprints.

## 6. STATEMENT OF PROBLEM

Society and Crimes are interrelated. A society without any commission of crime is a false belief. With digitalization of Indian society, the sudden rage of virtual world has brought about dynamic change towards adaptability conditions of individuals giving vent to crimes in cyber space to upsurge predominantly. Cyber crimes includes any type of crime that is committed in the cyber space using a computer-system and/or internet technologies which can be proved or disproved with the usage of viable digital footprints which are in the form of traces created instantly which are left behind by an individual when he starts browsing internet for any purpose Unfortunately there is a humongous gap between the law-enforcement and technology which

<sup>7</sup> Licklider, J.C.R. The Computer as a Communication Device. 1968.

Accessed 25 July 2019. Has stated that

In a few years, men will be able to communicate more effectively through amachine than face to face. That is a rather startling thing to say, but it is our conclusion.

<sup>8</sup> Gurumurthy, Anita. YES, NO, IT'S COMPLICATED Are India's Laws on Surveillance a Threat to Privacy? 28 Dec. 2018, 00:15 IST p. THE HINDU, www.thehindu.com/opinion/op-ed/are-indias-laws-on-surveillance-a-threat-to-privacy/article25858338.ece. Accessed 1 May 2022.

<sup>9</sup> Anand, Utkarsh. "Right to Privacy Case: Supreme Court Says Facebook Knows Our Friends, Uber Knows Our Location." CNN-News18, 25 Aug. 2017 11:47

IST, www.news18.com/news/india/hscap. Accessed 22 July 2019. Has discussed in detail about the usage of active and passive digital footprints as proofs for deciding cases which is inferred from Justice Sanjay Kaul inferences.

<sup>10</sup> Misra, Dipak. Ex CJI. Citizens shouldn't blatantly rely on Social Media: CJI Dipak Misra on Mob Lynching. 24 July 2018 19:45 IST, p. The Times of India, timesofindia.com, timesofindia.indiatimes.com/india/citizens-shouldnt-blattantly-rely-on-social-media cji dipak misra on mob lynching/articleshow/65121528.cms. Accessed

has created the sole issue to arise. The investigating officer have to be trained to overpower challenges in the process of collection and preservation of digital footprints and reproduction of same during legal proceedings complying to the Information Technology Act, 2000.

This study is attempting to signify the usage of digital footprints to be put forth as electronic evidences in new-age crime and gain recognition for digital footprints in legal proceedings. The research aims to help the investigating officer regarding the procedure of collection and preservation of digital footprints and reproduction of the same during legal proceedings which needs to be improved to impart equitable judicial conviction and to meet the meagerness of the present Information Technology Act, 2000.

In this study Odisha has been taken as sample area .With Digitalization and Odisha becoming internet hub there has been sudden rise of cyber crimes which cannot be equitably convicted due to the lacuna in Information Technology Act, 2000 constricting the legal enforcement officers in the matters regarding procedure of collection, preservation of digital footprints and reproduction of the same during legal proceedings which needs to be improved.

**7. RESEARCH METHODOLOGY**

This research includes an Exploratory Research Study of legal framework of India with laws of China, UK and US concerning the usage of digital footprints as evidences in Court of law which will help in facilitating conviction rate. The focus of this study is to emphasize the acceptability and significance of usage of digital footprints in legal proceedings in the current scenario of growing nature of crimes today which are being planned ventures with no physical footprint left behind that can lead to capture and custody. Therefore, given that even our smallest requirements are being fulfilled by the internet and web, digital footprints is a sure-shot way of pin-pointing guilt.

**Research Approach**–It is an Exploratory Research Study.

**Research Design**–The method of Post Test Design has been followed which has been inferred after the filled up questionnaires has been collected from the respondents whose responses are inevitable for proving our hypothesis correct in concluding that the usage of digital footprints by the Court will facilitate correct conviction in case of growing cyber crimes.

**Study Setting**–Baleswar, Cuttack, Ganjam, Khordha, Sundargarh

**Study Duration**–6 months

**Target Population**–The target population are the people having access to internet usage in Baleswar, Cuttack, Ganjam, Khordha, Sundargarh.

**Accessible Population**–The population accessed for this study are the respondents ranging within the age group of 15 years to 75 years.

**Sample Size**–The sample size consists of 360 respondents having access to internet residing at Baleswar, Cuttack, Ganjam, Khordha, and Sundargarh.

**Respondents**–The total number of sample respondents from whom filled up questionnaires are collected from is 360 respondents.

**These Respondents included**

*Table 1: Total Number of Sample Respondents.*

Respondents	Total Respondents
Cyber Crime Victims	250
Technocrats	50
Cyberand Other Lawyers	50
Law Enforcement Officials	10
Total	360

**8. DATA ANALYSIS**

This sample study will help us in visualizing the lacuna in the legal framework which is posing as a major hindrance in facilitating usage of digital footprints during court proceedings at a micro level Thus helping us in getting an insight over the problems being faced in its acceptance as evidences leading us to decipher the lacunas in Information Technology Act , 2000, making a comparative study possible with the legality of five major countries UK and US and China resulting in proving our hypothesis framed to be true.

*Table 2: Whether Usage of Digital Footprints by the Court Will Facilitate Correct Conviction.*

		Frequency	%	Valid %	Cumulative %
Valid	Yes	312	86.4	86.4	86.4
	No	48	13.6	13.6	100.0
	Total	360	100.0	100.0	

The Information Technology Act of 2000 has been consistently modified, with amendments made in

other Acts acting as percipients to keep a check on the growing old and innovative forms of crimes being

committed using digital platform and catering to meet the demands of continuous technological trends attempting to curtail those, that has attained

totally new stature requiring improved, appropriate, exhaustive, and well outlined regulation.

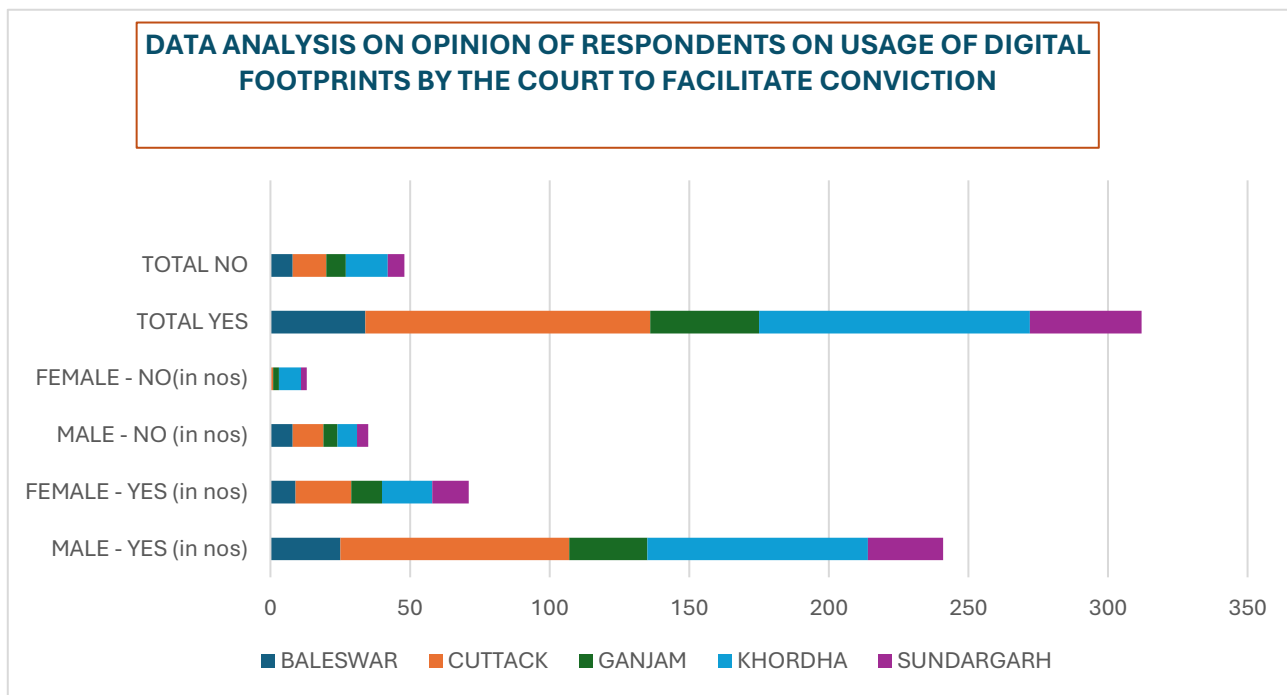


Figure 1: Digital Footprints Are Not Facilitating Conviction in Court Cases for Proving of Hypothesis.

It can be concluded from the above that the Hypothesis considered for this study to be true as it indicates that nearly 86.67 percent of total respondents have opined that usage of digital footprints by courts can facilitate conviction.

9. CONCLUSION

It can be inferred that digital footprints are being denied recognition in legal proceedings due to various reasons and is a matter of global concern.

It is observed from the study that young girls mostly encountered Online stalking and Identity theft while working women faced Online stalking, Identity theft, Money Swindling , Theft of Password(Hacking) and Fake Accounts on Matrimonial Websites. Men on the other hand mostly encountered Money Swindling, Theft of Password (Hacking) and to some extent Fake Accounts on Matrimonial Websites. Lack of Awareness amongst people and lack of technical and legal structure in putting a check over these forms of crimes being committed. There is legal lacuna for keeping

complete check over contents already present in the cyber world.

10. SUGGESTIONS

Justice S K Panigrahi has said about “improving the cyber intelligence, cyber forensics and cyber prosecution training that are long overdue for boosting the hitherto rickety” in *Shibani Barik v. State of Odisha, 2020 SCC OnLine Ori 425*<sup>11</sup> Digital platform are not bounded jurisdictionally and the sources of information are invariable basing upon servers existing in foreign countries which are posing as a major hindrance for the law enforcement officers in collecting data and information against perpetrators – Hon’ble Chief Minister of Odisha Shri Naveen Patnaik <sup>12</sup>

Ex Director General of Police (DGP) Abhay Kumar has stated that “The speed with which information, facts, allegations and rumor travels is very fast. Our response must match this speed. We should improve the expertise to solve the cyber crimes, which are very complex in nature”<sup>13</sup>

<sup>11</sup> Judgment imparted under point number 12 *Shibani Barik v. State of Odisha, 2020 SCC OnLine Ori 425*, decided on 28-05-2020

<sup>12</sup> Odisha CM inaugurates 14 police stations to investigate cybercrime, economic offences

<https://www.aninews.in/news/national/general-news/odisha-cm-inaugurates-14-police-stations-to-investigate-cybercrime-economic-offences20211230040848/>.

<sup>13</sup> Mohapatra, D. (2020). *Odisha DGP unhappy over poor investigation, high acquittal* | *Bhubaneswar News - Times of India*.

Though evidences in electronic format have been given permission for being accepted during legal proceedings legal framework in giving equitable recognition to such forms of evidences are still in nascent stage. Even though they are being accepted

as secondary and tertiary evidences still considering them as primary evidence are circumstantial in nature and cases involving various timelines are difficult to decide as legality of countries varies.

## REFERENCES

- Anand, Utkarsh. (2017, August 25). Right to Privacy Case: Supreme Court Says Facebook Knows Our Friends, Uber Knows Our Location. *CNN-News18*. "Has discussed in detail the usage of active and passive digital footprints as proofs for deciding cases, which is inferred from Justice Sanjay Kaul's inferences." <https://www.news18.com/news/india/hscap> [Accessed 22 July 2019].
- Arakerimath, Prof. Anjana R., & Gupta, Pramod Kumar. (2015). Digital Footprints: Pro, Cons and Future. *IJLTEMAS, Volume IV, Issue X, October 2015 Edition*. "Has discussed passive footprints." <https://www.ijltemas.in/DigitalLibrary/Vol.4Issue10/52-56.pdf> [Accessed 21 April 2020].
- Odisha CM Inaugurates 14 Police Stations to Investigate Cybercrime, Economic Offences. *ANI News*. <https://www.aninews.in/news/national/general-news/odisha-cm-inaugurates-14-police-stations-to-investigate-cybercrime-economic-offences20211230040848/>.
- WhatsApp to Sue Users Who Send Way Too Many Messages. *Financial Express*. <https://www.financialexpress.com/industry/technology/whatsapp-to-sue-users-who-send-way-too-many-messages/1606340/>.
- Impact of Digital Technologies. *United Nations*. <https://www.un.org/en/un75/impact-digital-technologies>.
- AfriPol – African Union. <https://afripol.africa-union.org/>.
- E-Transactions Legislation Worldwide. *UNCTAD*. <https://unctad.org/page/e-transactions-legislation-worldwide>.
- Policies for Harnessing Digital Data. (2019). *United Nations Conference on Trade and Development (UNCTAD), Digital Economy Report: Value Creation and Capture – Implications for Developing Countries*, Pg. xix.
- Serger, Alexander. (2019, November 20–22). Result of Capacity Building and Impact on Legislation. *Council of Europe, Cybercrime Division, Octopus Conference, Strasbourg*. Attended online webinar.
- Saraswat, V. K., Dr. Member, NITI Aayog. Cyber Security. Discussed at *Cyber Security Conclave, Vigyan Bhawan, Delhi*. Attended online.