VOL 8 | Issue 2| July-Dec 2024

ISSN : 2581-6837

jims

JIMS JOURNAL OF LAW

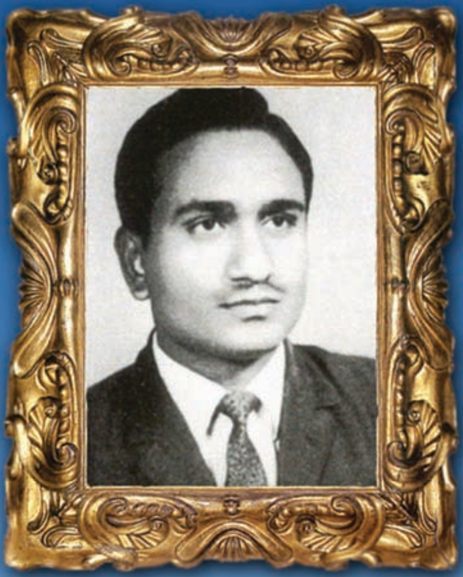
A Bi-Annual Peer Reviewed Journal

JIMS ENGINEERING MANAGEMENT TECHNICAL CAMPUS
48/4, KNOWLEDGE PARK III, Greater NOIDA 201308
www.jimsgn.org

A TRUE VISIONARY

"You see things and you say **Why?** *But I dream of things that never were and say* **Why** *not?"*

- George Bernard Shaw



Shri Jagannath Gupta
(1950 - 1980)

Also a true visionary...who dared to dream!
He lives no more but his dreams live on....and on!

JIMS (Rohini)	**-**	**1993**
JIMS (Kalkaji)	**-**	**1997**
JIMS (Vasant Kunj)	**-**	**2003**
JIMS (Jaipur)	**-**	**2003**
JNIT (Jaipur)	**-**	**2004**
JIMS (Greater Noida)	**-**	**2008**
Jagannath University (Jaipur)	**-**	**2008**
Jagannath University (Bahadurgarh)	**-**	**2013**

And more dreams to come!

Dr. Amit Gupta, Chairman, JIMS Group, **chairman@jagannath.org**

Editorial Office & Subscriber Service
JIMS Engineering & Management Technical Campus
48/4, Knowledge Park-III, Greater Noida, U.P. Phone #-01203819700,
lawjournal.gn@jagannath.org

From the desk of the Chief Editor

The landscape of legal discourse is constantly evolving, shaped by technological advancements, emerging jurisprudence, and the need for regulatory reforms. In this issue of our law journal, we present a collection of insightful articles that explore some of the most pressing legal challenges in the digital era. The contributions featured in this edition provide critical perspectives on cyber law, financial fraud, digital evidence, data privacy, artificial intelligence, and corporate taxation.

The advancement of Artificial intelligence necessitates legal scrutiny and *Towards Responsible AI: Legal Frameworks for Regulating Artificial Intelligence* discusses the regulatory challenges and the need for responsible AI governance to mitigate risks and ensure ethical compliance.

The paper on *The Role of Forensic Accounting in Financial Fraud Detection* delves into the significance of forensic accounting in identifying and mitigating financial fraud, emphasizing its role in modern financial regulations and compliance mechanisms.

The discussion on *Digital Evidence* provides an in-depth analysis of the admissibility, reliability, and challenges associated with digital evidence in judicial proceedings, a crucial topic in today's increasingly digitized legal landscape.

The right to privacy in the digital domain is a subject of intense debate, and *Exploring the Right to be Forgotten: Statutory Recognition and Challenges* addresses the legal complexities surrounding this right, shedding light on global legislative approaches and the challenges in its implementation.

The paper on *Legal Challenge of Cyberbullying and Online Harassment: A Comparative Study* examines the legal responses to cyberbullying and online harassment across different jurisdictions, highlighting gaps and recommending robust legal frameworks to ensure digital safety.

Lastly, *Corporate Tax Reforms in The Digital Economy: International Coordination and Challenges* critically assesses corporate taxation in the digital economy, exploring international efforts for coordination and the complexities that arise in taxing multinational digital enterprises.

Together, these contributions provide a comprehensive analysis of contemporary legal issues, offering valuable insights for academics, practitioners, and policymakers. I extend my sincere appreciation to the authors for their scholarly contributions and hope that this edition fosters meaningful discussions and advancements in legal thought.

Sincerely,

Pallavi

Prof. (Dr.) Pallavi Gupta
Thanking You

Table of Contents

TOWARDS RESPONSIBLE AI: LEGAL FRAMEWORKS FOR REGULATING ARTIFICIAL INTELLIGENCE

Ramandeep Singh
Research Scholar, Faculty of Law, Guru Nanak Dev University, Amritsar

Dr. Manjit Singh
Assistant Professor, Faculty of Law, Guru Nanak Dev University, Amritsar

ABSTRACT

With the advancement of technology, it has become possible to develop a human-like intelligence system, also called Artificial intelligence or AI. Artificial Intelligence is a machine learning mechanism that can replicate humans' responses in given circumstances. The ability of machines to think rationally like humans can pose infinite challenges to various sectors which have to be regulated. There is a need for a balanced approach to regulating artificial intelligence as comprehensive regulation should not restrict the achievement of the full potential of this technology but a complete lack of regulation could also be disastrous for human employment. It is important to regulate artificial intelligence to keep pace with the rapid transformation in technology. In this article, the author attempted to understand the concept of artificial intelligence, its applications and challenges in various sectors, the international regulatory framework, and the way forward.

Key words: *Artificial Intelligence, Automated Decision-Making, Legal Regulation, Machine Learning*

Introduction

In today's world, artificial intelligence (AI) is drastically altering how social relationships and transactions are structured. To make valuable decisions for society, AI systems and the algorithms underpinning them are becoming increasingly significant. Examples include clinical decision support systems that diagnose illnesses, policing systems that forecast the probability of criminal activity, and filtering algorithms that classify and offer users personalised content. Artificial intelligence (AI) differs from previous technologies in that it can replicate or compete with human intelligence in complicated problem-solving, as computers can accomplish many cognitive activities that humans have been performing better[1].

The idea of creating smart technology which is as intelligent as human beings is not a new concept but there are two different views on this technology. One is the pessimistic view, the believers of which consider artificial technology as the enemy of mankind and a threat to society as such intelligent and autonomous technology cannot be controlled by humans and the other is an optimistic view, which believes in its potential benefits for the betterment of human beings as such technology can perform the tasks which are not humanly possible. Either view cannot be ignored by giving more value to the other and both have to be harmoniously understood in different contexts and a balanced approach is required to regulate this technology[2]. The opinions on the impact of achieving human-level machine intelligence on humankind are opposites as the researchers regard that either it would give extremely good results or extremely bad results even extending to human extinction. Professor Nils Nilsson emphasized the concept of artificial general intelligence, which he believes to be a type of strong AI that can mechanize human-level intelligence. AI technology has not yet reached the level of abstract thinking and it relies upon the datasets of previous experiences to base its decisions in the decision-making process[3].

There are several risks associated with this technology such as lack of control, biases, discrimination, unemployment, breach of privacy, contravention of human rights, cybercrimes, espionage, interference in democratic processes etc., which should be understood in the deepest sense and mitigated with the help of a

[1] Araz Taeihagh, "Governance of artificial intelligence" 40(2) Policy and Society 137 (2021).

[2] Celal Hakar Kan, "Artificial Intelligence (AI) in the Age of Democracy and Human Rights: Normative Challenges and Regulatory Perspectives" 9(25) International Journal of Eurasian Education and Culture 146 (2024).

[3] Nick Bostrom, Superintelligence: Paths, Dangers, Strategies (Oxford University Press, United Kingdom, 2014).

regulatory framework. To take advantage of the benefits provided by AI, it is essential to define new moral responsibility attribution models and establish best practices for delegation in light of all those risks. Stakeholders who create and implement AI-based systems need to improve their understanding of the principles upheld by human rights and how those principles relate to their behaviour. Risk assessment methods can provide assistance and adaptability for Big Data and AI applications. The regulation of AI by the authorities must seek to protect the users from these risks and ensure compliance by the manufacturers of these applications[4].

Several questions arise with regard to the regulatory framework on artificial intelligence, for instance, firstly, whether the regulatory framework should be strict or self-regulatory in nature, secondly, whether the regulatory framework has to be vertical or horizontal in application, and thirdly, in what manner the regulatory framework be implemented consistently across all states.

What AI Regulation Denotes

In a general sense, the word 'artificial' implies the copy of something natural[5]. Artificial is something which is man-made and is not the result of any natural process. The word 'intelligence' has a wider meaning and it generally refers to the way we think and act. It implies rational behaviour in terms of the way we perceive, understand, predict and manipulate things. Intelligence may be perceived as internal thought processes and reasoning or external intelligent behaviour. Therefore, Artificial Intelligence is a man-made technology which can think rationally and act rationally as human beings. The thinking or cognitive abilities of AI include automated reasoning or decision-making, natural language processing, machine learning and knowledge representation. To understand the cognitive abilities of AI, it is required to understand that “rational thinking” is based on logic and probability. Logic is meant to derive a conclusion from given premises with inference where certain knowledge or information is required. But where there is no certain information available, the whole process of decision-making is based on probability. A thorough model of rational thought can be built using probability, which starts with basic perceptual data and leads to an explanation of the functioning of the world and future predictions. The ability to “act rationally” by AI systems includes autonomous operation, perceiving the surroundings, adapting to change and, setting and achieving goals. In this context, an AI system is referred to as a rational agent, which acts to achieve the best results or where the information is not certain, the best possible results[6].

There are several definitions of the term 'regulation' provided in the textbooks. Firstly, “regulation is the promulgation of rules by the government accompanied by mechanisms for monitoring and enforcement, usually assumed to be performed through a specialist public agency. Secondly, “regulation means any form of direct state intervention in the economy, whatever form that intervention might take.” Lastly, “regulation refers to all mechanisms of social control or influence affecting all aspects of behaviour from whatever source, whether they are intentional or not.” From the above definitions, it can be concluded that regulation means a legal instrument used to exercise control on the subject matter by the authority. Here, the subject matter of regulation is AI technology. Thus, AI regulation denotes the control of the state over the manufacturing, consumption and management of AI applications, whether it involves sanctions for ensuring its compliance[7]. Article 13 Clause 3(a) of the Indian Constitution provides that “law” includes any ordinance, order, by-law, rule, regulation, notification in the territory of India of the force of law[8]. However, the term 'regulation' is not defined in the Constitution but it is included in 'law' made by the state. Here, the term 'State' is defined by Article 12 of the Constitution which provides that 'state' includes the Government and Parliament of India and the Government and the Legislature of each of the States and all local or other authorities within the territory of India or under the control of the

[4] Patricia Gomes Rêgo de Almeida, Carlos Denner dos Santos, et.al., “Artificial Intelligence Regulation: a framework for governance” 23 Ethics and Information Technology 506 (2021).

[5] ARTIFICIAL | English meaning - Cambridge Dictionary

[6] Stuart J. Russel and Peter Norvig, Artificial Intelligence: A Modern Approach 19-22 (Pearson Education Limited, United Kingdom, 4th Edition).

[7] Julia Black, “Critical Reflections on Regulation” 27 *Australian Journal of Legal Philosophy* 11 (2002).

[8] The Constitution of India, art 13.

Government of India[9]. Hence, regulation means the legislative action taken by the legislative or executive bodies of government including delegated legislation. In State of Tripura & Ors vs Sudhir Ranjan Nath[10], the Hon'ble Supreme Court observed the word 'regulation' has a wider meaning according to the context and it cannot be given a rigid or inflexible meaning. It cannot be used synonymously with the word 'prohibit' as it does not have a restrictive meaning but it implies the power to rule, direct or control, and involves the adoption of a rule or guiding principle to be followed, or the making of a rule with respect to the subject to be regulated.

Therefore, AI regulation refers to the power of the state authority to control all aspects of AI technology but it is not meant to completely prohibit the operation of this technology. The strict or self-regulatory nature of the regulation is decided by the concerned state authority as it is a matter of sovereignty unless there is a global consensus between the states in this regard.

Fundamentals of AI

Artificial Intelligence

The term 'Artificial Intelligence' was coined in 1956 by John McCarthy. There has been no universally accepted definition of AI but it is associated with various concepts such as smart systems, intelligent systems, autonomous systems, AI agents, AI algorithms etc. The High-Level Expert Group of the European Commission defines AI technology as “software systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing the environment by their previous actions.”[11]

Various authors have defined AI as a software system which can mimic human thinking processes on any digital device such as automated vehicles, smartphones, smart home appliances etc. Stuart Russel and Peter Norvig have given two approaches to AI systems; one related to the thinking process (rational thinking) and the second related to the behaviour (rational act). Prof. Dr. George F. Luger defines AI as “a branch of information technology science related to automation of human behaviour.” According to the International Dictionary of Artificial Intelligence, AI is “a system concerned with rapidly developing techniques to allow computers to act in an intelligent manner, such as a human would.” The given definitions suggest that AI is a technology with intellectual skills, which can comprehend, learn and autonomously make decisions without the influence of the will of the developer or the user[12].

Machine Learning

Machine learning (ML) and artificial intelligence are often confused as similar but it is a branch of AI technology. ML enables AI applications to learn behaviour patterns and responses to the given stimulus with the help of prior experiences. It is the most important characteristic of AI which helps it to improve its performance with prior experiences. Large datasets are used for initial input to the AI system before the first deployment, but later it can learn the decision-making process on its own with the help of different forms of ML. There are various forms of ML such as supervised learning, unsupervised learning and reinforcement learning[13]. Supervised learning refers to the process of learning with the help of datasets with labelled and well-defined objectives and expected

[9] The Constitution of India, art 12.

[10] AIR 1997 SUPREME COURT 1168

[11] *Supra* Note 4.

[12] Paulius Cerka, Jurgita Grigiene, et.al., “Is it possible to grant legal personality to artificial intelligence software systems?” 33 *Computer Law & Security Review* 687 (2017)

[13] Nicole Beltran, *Artificial Intelligence in Lethal Autonomous Weapon Systems – What's the problem?* (2020) (Unpublished Master's Thesis, Uppasala Universitet)

outcomes for training and testing the performance of the algorithms. Unsupervised learning refers to the process of learning with the help of unlabelled datasets for training and testing the performance of the algorithms. Principal Component Analysis (PCA) and Clustering are major techniques of unsupervised learning[14]. Reinforcement learning involves the use of reward and punishment as reinforcement for positive and negative outcomes. Positive and negative reinforcement affects the future responses and relevance of the given stimulus[15].

Narrow v General AI

AI can be classified into 'narrow' and 'general' AI based on its capability to perform tasks. Narrow AI is also referred to as 'weak' AI for its capability to perform a limited number of tasks of a repetitive or routine nature. General AI is also called 'strong' AI for its ability to think abstractly and set up and achieve determined goals autonomously. General AI is the form of AI which achieves human-level machine intelligence. Narrow AI can perform various tasks such as computer vision, natural language processing and speech recognition. Computer vision enables the systems to perform tasks such as segregating pictures, face recognition, determining facial emotions, predicting the body postures etc. The Natural Language Processing feature helps in detecting emotions from text, translation, chatbots, sentiment analysis and converting expressions in another language without altering their meaning. Speech recognition feature enables the system to analyse human speech. In these tasks, the narrow AI can even surpass human performance[16].

Risks associated with AI

Identifying and understanding the risks associated with AI technology is imperative for framing the regulatory policies and governance framework. The regulatory framework on AI has to balance the potential benefits and risks generated by this technology. The rapid pace of adoption of AI technology brings new risks which are the prime focus of governments to mitigate. The risks related to AI may be classified based on the desirability of consequences such as undesired risks including discrimination, bias, violation of privacy, misinformation, liability issues, unemployment etc., whereas the desired risks may include fake news, cybercrimes, manipulation of people, deep fakes etc[17].

Corner Cases

Corner cases refer to unexpected situations which the AI systems cannot handle due to lack of training to respond in what manner in such situations. The developers of the AI systems cannot anticipate all possible situations that may arise in their operation. Even though AI systems undergo various safety protocols, the unpredictable responses to identical datasets enhance the complexity of generalizing the decision-making process. The users of AI systems show less cautious behaviour while using them due to the automation bias and objective nature of such systems, which in some cases proves to be hazardous. For instance, the unique environmental conditions caused misinterpretations of Tesla's automated vehicles in the trial stage which led to fatal accidents[18].

Bias and Discrimination

The lack of transparency in the decision-making process of AI systems makes it difficult to understand the possible reasons for discrimination and bias. There are several reasons for such bias and discrimination which are categorized by Barocas and Selbst into five major reasons; firstly, the manner of defining the target variable or class labels, secondly, discriminatory effects in labelling the training data, thirdly, discriminatory effects in the

[14] Ibrahim Goni, Jerome Mishion Gumpy, et.al., “Cybersecurity and Cyber Forensics: Machine Learning Approach” 5(4) Machine Learning Research 48 (2020).

[15] Priya Pedamkar, what is Reinforcement Learning, retrieved from: What is Reinforcement Learning? | Function and Various Factors (Last accessed on Jan 24, 2025).

[16] *Supra* note 2.

[17] *Supra* note 4.

[18] *Supra* note 1.

collection of data sample, fourthly, the selection of certain features or attributes itself discriminate others without such features and lastly, the problem of proxies in which the bias may arise for membership in particular class due to certain protected characteristic which is otherwise relevant for rational and well-informed decisions. Apart from these reasons, the discrimination may be intentional by prejudicing the training datasets by the developer to produce discriminatory outcomes[19].

Determination of Liability and Responsibility

The determination of liability in the case of damage caused by automated AI systems is a critical question as to whether the owner or the manufacturer of the AI system would be made responsible for compensating the damage. In automated AI systems, the system operates independently of the will of the user or developer in their decision-making process, therefore, making the user or developer liable for the acts done by the automated AI system beyond their control is not an easy task. The UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts has provided an explanation of Article 12 which states the principle that responsibility lies upon the person on whose behalf the machine was programmed to perform the task. Article 12 extends to the AI agent system but does not cover the automated machine which operates autonomously without the control of the user. In autonomous systems, it is not possible to determine the cause of the errors and the person responsible for the errors. If the legal framework on AI systems makes the producers, developers and programmers of AI-based applications responsible for the errors arising from the automated systems, it would hamper the development of the technology. The product liability principle cannot be made applicable to AI-based applications because of unpredictability and lack of human control in their decision-making process[20].

Violation of Privacy

The AI-based applications are fully data-driven and have to be trained with huge amounts of data which could also include personal data of the persons even without their consent. The personal information may include personal health information and other personal information from which the system could re-generate even if removed or deleted after completion of the training the system. However, the data cannot be completely removed because the AI-based systems are not programmed to forget the information completely. The information once seen cannot be unseen. There is a huge risk of personal information related to a person being disclosed by the AI system to others. Moreover, AI systems can also generate incorrect personal information due to their training with huge amounts of data which has to be compressed to generate the output losing details of the information, which may sometimes produce incorrect information due to hallucinations and the AI systems are mostly trained with the purpose of generating the plausible outputs without having regard to the accuracy. For instance, an Australian attorney named Max Schrems sued OpenAI for providing his incorrect date of birth and failure to correct his personal information even after several requests[21].

Unemployment

In the Future of Jobs Survey Report 2025 by the World Economic Forum, 86% of the respondents expected that Artificial Intelligence is expected to transform the business trends by 2030. The rapid pace of adoption of AI technologies to enhance productivity comes along with unknown risks. The focus on leveraging these technologies in various industries must be to enhance the skills and performance capabilities of human Workers rather than substituting them. The technological development would result in the increase of inequality and unemployment in the absence of an appropriate regulatory framework, economic incentive structure and decision-making framework[22].

[19] Prof. Frederik Zuiderveen Borgesius, "Discrimination, Artificial Intelligence, and algorithmic decision-making" 15-23 (2018).

[20] *Supra* note 12.

[21] Leigh Wickell, "Privacy Harms in the AI Age: Time for a System Update" 11-13 Transparency Coalition (2024) retrieved from: PrivacyHarms-11+ (1).pdf (Last accessed on 26 January 2025)

[22] World Economic Forum, "Future of Jobs Report 2025" 10-12 (2025).

Role of European Union in Global AI Regulation

The AI regulation proposed by the European Union (EU) has attained a remarkable global status. The EU has emerged as a global leader in the field of digital sovereignty for the members as well as non-member state parties. Article 2 of the EU Regulation 2016/679 extends the scope of the regulations to the AI service providers located within the Union and the users located in third countries as well as the AI service providers and users both located within the third countries provided that the output of the AI service must be used in the Union. Hence, the scope of this EU regulation extends beyond the Union. The proposed regulation adopted a horizontal approach for general application in all sectors such as healthcare, finance, IT etc., instead of dealing with specific problems or particular gaps in the legal framework. The regulations are framed having regard to the present and future aspects of AI technology. Among the four areas covered by the EU normative structure to create a single digital market, the areas of our concern are, firstly, the protection of personal data through the General Data Protection Regulation (GDPR) and secondly, the regulation of Artificial Intelligence[23].

General Data Protection Regulation (GDPR)

GDPR was introduced by the EU in 2016 and came into force on May 25, 2018, to ensure the data privacy and protection of other rights of European citizens. However, the scope of GDPR extends beyond Europe to cover the subjects of this regulation living worldwide. The AI-based automated systems are data-driven and require a large number of datasets which also include personal data for training algorithms or in the cyber threat intelligence sharing process. GDPR allows the legitimate use and processing of personal data by the controller. Under this regulation, the 'Controller' has the authority to decide the use and means to process the data. What constitutes 'personal data' is a relevant question, which is the subject matter of this regulation. Article 4(1) of GDPR defines 'personal data' as “any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. Personal data includes any information from which a person or entity can be identified such as email addresses, usernames, payment transactions, IP addresses etc[24].

Certain rights, including the right to consent, the right to be forgotten, the right to an explanation, and the right to data portability, have been granted to data subjects in order to protect their privacy. To guarantee these rights for the data subjects, AI system developers, producers, and programmers must be able to afford sufficient adherence to GDPR standards[25].

Right to Consent – GDPR prohibited the use of the personal information of the data subject without his consent. The term 'consent' is defined by Article 4(11) as “consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”[26] Article 7 outlines the requirements for consent, one of which is that the controller must be able to prove the data subject's agreement to the use of personal data. Additionally, the data subject is free to revoke consent at any moment[27]. Recital 32 provides that the consent may be signified by written statement including by electronic means or by oral statement. Mere clicking on the pop-up option choosing technical settings, browsing a website, or engaging in any other behaviour with the intention to indicate the acceptance of the proposal to process the personal data of the data subject. However, the inactivity or silence of the user and pre-ticked boxes shall not be treated as consent. Recital 33 provides that the data subject can define the extent to which his personal information can be used.

[23] Guisella Finocchiaro, “The regulation of artificial intelligence” 39 *AI & SOCIETY* 1963 (2024).

[24] Brandon W. Jackson, “Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulations and Autonomous Network Defense” 21(1) *Minnesota Journal of Law, Science & Technology* 187-190 (2020).

[25] *Ibid.*

[26] General Data Protection Regulation 2016, art. 4(11).

[27] General Data Protection Regulation 2016, art. 7.

Recital 42 provides that the burden to prove the consent to be free and without unfair means is upon the controller.

Right to be Forgotten – Article 17 of GDPR provides the right of erasure of personal data to the data subject. The controller shall erase the personal data of the data subject upon his request without undue delay on the grounds of completion of the purpose for which the data was required, withdrawal of consent, objection of data subject to the processing, unlawful processing of the data, mandate of erasure of data for compliance of law of state to which the controller belongs and collection of data by information society service. There are certain exceptions to the right of erasure in which the controller is not obliged to remove the data such as the necessity to process the data in exercising the right to free speech and expression, according to legal requirements, serving the public interest, using the controller's official power, serving the public interest in matters of public health, or using statistics, scientific, or historical research or to support or defend the legal claims by the controller[28].

Right to an explanation – The right of data subjects to an adequate explanation for the decision-making process with their data is another important measure to ensure data privacy. Article 22 of GDPR provides for the right against using personal data to produce legal ramifications or influence the data subject with a judgment based on automated processing including profiling. It also provides some exceptions where the decisions are necessary to give effect to the contract between the controller and data subject, mandated by the law of the state to which the controller belongs or with the explicit consent of the data subject[29]. Recital 71 provides that profiling means the legal effects created by the automated decision-making process in which the personal data of the subject is processed by the automated system to evaluate to analyse the personal aspects of a natural person such as health, personal interests, work performance, financial condition etc. In automated decision-making, the explainability of the decision is a daunting task.

Right of Data Portability – Article 20 of GDPR ensures that the data subjects have the right to receive and send machine-readable versions of their personal information from one controller to another, as long as they have given their consent for automated processing. Direct data transmission between controllers may be made available to the data subject[30].

Regulation on Artificial Intelligence

The AI Regulations were proposed in 2021 which the European Parliament approved in June 2023 with certain modifications[31]. The AI regulation adopted by the EU is based on risk management which is commended for making efforts to identify and understand the risks associated with AI systems. This regulation is generally applicable to common problems or risks of AI applications in different sectors. It classified the risks of AI systems into three classes; unacceptable level, high level and low level of risks. Firstly, the unacceptable level of risks to the individual users or the society by the AI systems is controlled by a complete ban or prohibition of the system. Secondly, the high-level risks are controlled with detailed provisions of the regulation. In case of AI systems creating high risks, the developers of such systems must follow the prescribed procedure of CE certification and must adopt the standards for ensuring the quality of the datasets used for training, testing and validation purposes. To make such systems transparent, the events occurring during the whole lifecycle of the systems must be automatically registered. Such systems have to be designed with machine-human interfaces to enable their supervision by humans to prevent or minimize the risks to health, safety and fundamental rights. Thirdly, the low-risk creating AI systems must follow the codes of conduct and transparency obligations. The human subjects interacting with such systems must be given intimation that the system is based on AI technology and the manner of their operation must also be informed. In the case of AI technology capable of creating accurately resembling images, video or other multimedia content must indicate that the content is AI-generated[32].

[28] General Data Protection Regulation 2016, art. 17.

[29] General Data Protection Regulation 2016, art. 22.

[30] General Data Protection Regulation 2016, art. 20.

[31] *Supra* note 2.

[32] *Supra* note 23.

Article 5 of the Regulation on Artificial Intelligence of the European Parliament and the European Council 2024/1689 provides that the unacceptable risks include:[33]

(a) subliminal techniques causing manipulation or deceptive behaviour impairing the ability to make informed decisions by any person or other vulnerable persons due to youth, impairment, or certain social or financial situations.

(b) Social scoring or classification of the people as per their social behaviour, and personality characteristics resulting in detrimental or unfavourable treatment.

(c) Prediction of criminal behaviour of persons based on profiling or personality traits and characteristics.

(d) Increasing the size of facial recognition databases by arbitrarily grabbing facial image data from CCTV or the internet.

(e) Employing biometric data to classify natural persons to determine their race, political opinion, membership in trade union, religious or philosophical beliefs and sexual orientation and experiences.

(f) remote biometric identification systems for law enforcement in real-time in public areas.

Article 6 of the AI Regulation provides that the AI system covered by Annex I of the Union harmonisation legislation, as a product having the safety component or whose safety component is required to undergo compliance by third-party evaluation. Apart from these products, the AI systems mentioned in Annex III will also be regarded as high-risk.

Article 52 defines limited risk systems as those that create or modify pictures, audio, or video content, such as chatbots, biometric classification systems, emotion recognition systems, and deep fakes. Article 3(33) defines biometric data as personal information derived from particular technical procedures of a natural person's physical, physiological, or behavioural traits, such as fingerprint or face image information, that uniquely identify that individual. There are fewer transparency requirements for systems with limited risk. Administrative fines may be imposed for breaking these duties[34].

INDIAN POSITION ON AI REGULATION

In Justice K.S. Puttaswamy (Retd.) vs Union of India (2017)[35], the Hon'ble Supreme Court of India declared Article 21 of the Indian Constitution guarantees the right to privacy as a basic right. As a fundamental component of the rights to life and personal liberty, the right to privacy is subject to the same limitations as the freedoms enshrined in Part III.

The National Strategy for Artificial Intelligence released by NITI Aayog in June 2018, the think tank of the government of India observed the need for a legal framework for the protection of personal data and to move forward to make the AI responsible. To ensure the data privacy, ethics, safety and security of the AI domain, Indian lawmakers have to address the following requirements;[36]

a. Developing a data protection framework with adequate legal sanctions.
b. Developing regulatory frameworks for particular AI sectors.
c. Adoption of international standards in framing national data protection and privacy laws.
d. Compliance with international standards on data protection by the AI system developers.
e. The Self-regulatory nature of the laws rather than a strict legal burden.
f. Creating awareness among the masses for data privacy.

[33] Regulation (EU) on Artificial Intelligence 2021, art. 5.

[34] *Supra* note 2.

[35] AIR 2018 SC (SUPP) 1841.

[36] NITI Aayog, "National Strategy for Artificial Intelligence" 85-89 (2018).

In August 2022, the Digital Personal Data Protection Bill was introduced in parliament in line with the General Data Protection Regulation (GDPR) of the EU which became an act by receiving the assent of the President of India in August 2023 but it has not yet come into force as the Government of India has not notified in it the official Gazette. The major provisions of this legislation include; establishing the Data Protection Board of India (DPBI) which shall be the single regulatory body for the processing of personal data of citizens, exceptions allowing the government to process personal data for investigation of offences, fair and reasonable use and the protection of sovereignty and integrity of India, designation of Significant Data Fiduciaries (SDFs) with independent data auditor and data protection officer, and punishments for the violation of obligations. The purpose of this legislation is to protect the personal data of the citizens from processing unlawfully and to ensure their right to privacy. It does not specifically deal with the regulation of AI but indirectly deals with the challenge of data privacy by mandating compliance by developers, manufacturers and programmers of AI services designated as data fiduciaries under this act for processing personal data to train, test and validate their AI products and services.

Conclusion

The challenges apparent with the massive adoption of AI to bring technological transformation to society demand a regulatory framework which provides standards, guidelines and mechanisms for the development and deployment of AI services. The challenges posed by AI include data privacy, bias and discrimination, uncertainty regarding liability and responsibility for damages, lack of control in the automated processing of data etc. The decision-making process in the majority of AI applications is opaque or non-transparent resulting in a lack of predictability and explainability of its decisions. The question of treating AI-based applications as products or vesting them with the legal personality to determine the liability for damages occurred due to errors in automated decision-making. In the context of AI regulation, the European Union has played a significant role in providing comprehensive legal regulation for the global digital market. Apart from the EU, various international organizations have enacted regulations for different areas of the AI domain and several countries such as the USA and China have enacted designated laws for the regulation of AI applications. India still has no designated legislation on regulation of AI but the Digital Data Protection Act 2023 mandated data privacy by developers of AI applications. There is a need for international cooperation in the regulation of AI systems due to their transnational operation.

THE ROLE OF FORENSIC ACCOUNTING IN FINANCIAL FRAUD DETECTION

Dr. Shweta Yadav
Assistant Professor, Ishan Institute of Law, Greater Noida

ABSTRACT

The manuscript presents a comprehensive analysis of forensic accounting methodologies, investigative techniques, and the regulatory landscape that governs financial fraud detection. Given the increasing complexity of financial crimes, this study provides relevant discussions on how forensic accounting contributes to legal proceedings and enhances transparency within financial institutions. This paper aims to explore the critical role of forensic accounting in identifying, preventing, and mitigating financial fraud, offering valuable insights into its significance in corporate governance and financial integrity.

Introduction

Forensic accounting began as a way to look into financial fraud and other related wrongdoings, and it has since shown its importance in the financial world. As the risk of fraud in companies has grown, so has the demand for skilled forensic accountants. In India, the increasing threat of financial fraud and mismanagement has negatively impacted businesses, investors, and the general public. The country has seen a variety of financial crimes, from embezzlement and tax evasion to corporate fraud and money laundering. There is now a greater need than ever to have strong systems in place to detect, investigate, and prevent these types of frauds and scams.

Overview Of Forensic Accounting and Financial Fraud in India

Fraud has grown to be a major problem for companies and organizations all over the world in recent years, and India is no different. An organization's reputation, stakeholder confidence, and financial health can all suffer significantly as a result of financial fraud. As a result, businesses are using forensic accounting more frequently to identify, stop, and lessen the effects of fraud. To find financial abnormalities, such as fraud, embezzlement, and money laundering, forensic accounting is a specialist area that blends accounting, auditing, and investigation skills. For businesses, it is an effective tool for looking into, identifying, and taking proper action against fraudulent actions. The role of forensic accounting in identifying and stopping fraud in particular Indian organizations will be the main focus of this study.

The term forensic accounting refers to the application of specific accounting principles to the identification, investigation, and prevention of financial misconduct and disputes. This has particular significance for India where there has been dramatic growth of the financial sector and increased incidence of fraud. Forensic accountants investigate complex financial transactions, identify anomalies, and prepare reports that may serve as evidence in a court of law. Forensic accounting as a sub-discipline of accounting is specific to the investigation and evaluation of fraud, embezzlement and other financial misconduct. Working frequently with law enforcement or legal teams, forensic accountants collect and examine evidence about financial crimes using their expertise in accounting and auditing as well as investigative methods[1].

Research Objectives

Research on *The Role of Forensic Accounting in Financial Fraud Detection* generally aims to achieve several core objectives. Here are some common objectives you could consider:

a) **Understanding Forensic Accounting Techniques:** Explore the methods and tools forensic accountants use to

[1] Uplift Team, 'Forensic Accounting & Its Job Scopes in Global and Indian Backdrop' (Uplift PRO Blog, 23 October 2024) <https://www.upliftprofessionals.in/blog/2024/10/forensic-accounting-scope-in-global-and- india/>

detect, investigate, and prevent financial fraud. This might include analysis of auditing techniques, data analytics, and investigative procedures specific to forensic accounting.

b) **Identifying Types of Financial Fraud:** Examine different types of financial fraud such as asset misappropriation, corruption, and financial statement fraud, to understand how forensic accounting can detect each one effectively.

c) **Assessing the Effectiveness of Forensic Accounting in Fraud Detection:** Evaluate the impact of forensic accounting on fraud detection within organizations, including how it improves financial oversight and reduces fraudulent activity.

d) **Highlighting the Role of Technology in Forensic Accounting:** Investigate how advancements in technology—such as AI, data mining, and blockchain—are integrated into forensic accounting practices to detect and prevent fraud more efficiently.

e) **Examining Challenges Faced by Forensic Accountants:** Analyze the challenges forensic accountants face, such as access to data, regulatory barriers, and technological limitations, and explore potential solutions.

Hypothesis

Forensic accounting significantly enhances the accuracy and reliability of financial fraud detection within organizations. Organizations that employ forensic accounting techniques experience lower incidences of financial fraud compared to those that rely solely on traditional accounting practices. The integration of advanced technology in forensic accounting, such as data analytics and artificial intelligence, increases the efficiency of fraud detection and reduces investigation time. Forensic accounting is more effective in detecting specific types of financial.

fraud, such as financial statement fraud and asset misappropriation, than traditional auditing methods. The presence of trained forensic accountants in a company's financial team positively correlates with stronger internal controls and reduced financial risk. The lack of a standardized regulatory framework limits the effectiveness of forensic accounting in fraud detection across different industries. Forensic accounting contributes to improved corporate governance practices, resulting in higher stakeholder trust and transparency.

These hypotheses can be used as a basis for empirical testing and analysis to assess the specific impact and value forensic accounting brings to financial fraud detection.

Statement of Problem

Financial fraud has become increasingly complex and widespread, posing significant threats to businesses, investors, and the economy as a whole. Traditional accounting and auditing practices are often insufficient in identifying sophisticated fraud schemes, leaving organizations vulnerable to financial manipulation, asset misappropriation, and other forms of fraud. As a specialized field, forensic accounting applies investigative techniques and advanced analytical tools to detect, prevent, and investigate financial fraud. However, despite its potential, the role and effectiveness of forensic accounting in mitigating fraud remain under- explored in many sectors, particularly concerning the integration of modern technologies, the challenges faced by forensic accountants, and the impact on corporate governance.

The problem lies in the lack of comprehensive understanding and empirical data on how forensic accounting can be best utilized to detect financial fraud effectively. Furthermore, the regulatory inconsistencies and absence of standardized practices in forensic accounting hinder its adoption and efficacy in organizations. This study seeks to address these gaps by examining the role of forensic accounting in financial fraud detection, assessing its impact on fraud prevention, and identifying factors that influence its effectiveness in different organizational settings.

Key Aspects Of Forensic Accounting

a. **Fraud Detection:** Forensic accountants investigate discrepancies in financial records to detect fraudulent activities, such as asset misappropriation, financial statement fraud, and corruption.

b. **Investigation:** Beyond examining financial statements, forensic accountants may delve into background checks, interviews, and digital records to build a complete picture of any suspicious financial activities.

c. **Litigation Support:** Forensic accountants often assist in legal cases, providing expert testimony and reports that can be used as evidence in court. They help lawyers and law enforcement understand complex financial data and provide an objective assessment of financial misconduct.

d. **Quantifying Damages:** In civil cases, forensic accountants can help determine financial losses caused by fraud or mismanagement, which is crucial for legal settlements or insurance claims.

e. **Forensic Tools and Techniques:** They employ various tools like data analytics software, ratio analysis, and digital forensics to track irregularities and unusual patterns in financial data.

Importance of Forensic Accounting

The integrity of financial systems depends on forensic accounting, particularly in areas with complicated regulatory frameworks or high rates of financial fraud. In today's intricate economic and regulatory landscape, forensic accounting is essential to preserving financial systems' accountability, transparency, and confidence. Its significance is multifaceted and provides significant advantages to the legal system, regulators, and organizations[2].

The following explains why forensic accounting is essential:

1. Detecting and Preventing Financial Fraud

Forensic accountants are skilled in identifying irregularities and potential fraud schemes, such as embezzlement, bribery, money laundering, and financial statement manipulation. By detecting fraud early, they help organizations avoid financial losses and reputational damage. They also establish internal controls and recommend risk mitigation strategies, which can prevent future fraud.

2. Supporting Legal Proceedings and Litigation

Forensic accountants play a vital role in legal cases, such as disputes involving fraud, breaches of contract, bankruptcy, and shareholder lawsuits. They provide expert testimony, evidence, and analysis that help courts understand complex financial issues. Their expertise is critical for calculating damages, assessing lost profits, and supporting claims in financial disputes.

3. Strengthening Corporate Governance

Better corporate governance is facilitated by forensic accounting, which guarantees financial accountability and transparency. Forensic accountants assist in locating conflicts of interest, unethical behaviour, and inadequate internal controls that may compromise the accuracy of financial reporting by examining financial data.

4. Assisting Regulatory Compliance

Regulations that organizations must comply with include financial reporting requirements, anti-money laundering (AML) rules, and anti-bribery and corruption (ABC) standards. By identifying and resolving non-compliance concerns, forensic accountants contribute to the assurance of adherence to these standards. This

[2] *Ibid.*

lessens the possibility that regulatory violations may result in fines, legal penalties, and damage to one's reputation.

5. Safeguarding Public Interest

By exposing fraud and other financial wrongdoings in governmental entities, public institutions, and nonprofits, forensic accounting upholds public confidence. To safeguard taxpayers, investors, and benefactors, forensic accountants look into and disclose financial misconduct. In situations involving public funds or welfare, where financial wrongdoing can have far-reaching effects, their position is vital.

6. Providing Confidence to Investors and Stakeholders

Forensic accounting helps creditors, investors, and other stakeholders feel more confident in a company environment characterized by financial scandals. Forensic accountants provide stakeholders with assurances about the organization's integrity by confirming the correctness of financial accounts and looking into potential fraud. This is especially helpful in audits, mergers, and acquisitions when investors need precise financial data to make wise choices.

7. Facilitating Insurance Claims and Loss Recovery

Forensic accountants help evaluate insurance claims, including those related to liability, employee theft, and business interruptions. They aid in validating losses and calculating precise claim amounts, which streamlines and increases the transparency of the claims process. By tracking down stolen assets and supporting asset recovery procedures, they also aid in loss recovery operations.

8. Adapting to Technological Advancement

To combat emerging types of digital fraud, forensic accounting has developed in tandem with the growth of digital finance, online transactions, and cryptocurrencies. In the current financial environment, forensic accountants are valuable because they use cutting-edge methods like blockchain analysis, artificial intelligence, and data analytics to follow intricate fraud schemes. This flexibility guarantees that businesses can react to emerging fraud threats.

ix. Building a Culture of Integrity and Accountability

Within enterprises, forensic accounting promotes a culture of moral conduct and responsibility. It motivates staff and management to uphold high ethical standards by aggressively looking into wrongdoing and placing a strong emphasis on open reporting. Better decision-making, a lower rate of fraud, and an improved reputation for the company can result from this. A vital part of contemporary financial management and fraud prevention is forensic accounting. Forensic accountants safeguard financial systems, enforce the law, and promote the moral integrity of businesses by fusing their knowledge of accounting with investigative abilities[3].

7. Procedure For Examining Financial Misconduct And Fraud

Finding financial fraud and misbehaviour requires several procedures in the forensic accounting investigation process. Usually, these actions consist of:

1. Evidence Collection: Forensic accountants collect relevant financial documents, records, and other evidence to guarantee a complete understanding of the case.

2. Data analysis: Advanced data analysis techniques, such as forensic software tools, are used to look into financial transactions, identify trends, and identify anomalies.

[3] Dr Percy Bose B ‘Role of Forensic Accounting in India' (2023) 2456-4184 IJNRD <https://www.ijnrd.org/papers/IJNRD2303210.pdf>

3. Interviewing Parties: Those involved in the case are interviewed by forensic accountants to gather further information and insights.

4. Reporting: After conducting a thorough investigation, forensic accountants provide in- depth reports detailing their findings. These reports may include recommendations for legal action, evidence of fraud or misconduct, and financial damages.

In *Satyam Computer Services Scandal* (2009): The Satyam case, one of the biggest business scandals in India, concerned Ramalinga Raju, the founder of the company, manipulating accounts to inflate assets and income. To expose the falsified bank statements and exaggerated sales figures that misled authorities and investors, forensic accounting was essential. A weakness in internal controls was revealed by the investigation, which increased awareness of the value of forensic procedures in corporate governance[4].

In *Nirav Modi-PNB Scam* (2018): Businessman Nirav Modi is accused of masterminding a $1.8 billion scam involving improper Letters of Undertaking (LoUs) from PNB in this notorious case. A complex web of sham corporations and dishonest financial activities was exposed by forensic accountants who tracked money across multiple nations. The case demonstrated the necessity of thorough forensic accounting to identify financial malfeasance early on and stop widespread harm[5].

In *IL&FS Crisis* (2018): Massive financial irregularities and poor debt management were part of the Infrastructure Leasing & Financial Services (IL&FS) crisis. Executives at IL&FS had lied about the company's financial situation, taken on excessive debt, and transferred money into shell companies, according to forensic auditors. This case demonstrated how forensic accounting can reveal operational irregularities and inadequate governance in major financial organizations[6].

In *Vijay Mallya and Kingfisher Airlines* (2012): Former Kingfisher Airlines chairman Vijay Mallya was charged with embezzling more than ₹9,000 crores (about $1.2 billion) in loans from Indian banks. Allegedly, the money meant for Kingfisher Airlines was transferred to Mallya-owned shell corporations. Using financial tracing methods and document analysis, forensic accountants were able to track down the diversion of loan proceeds. They discovered a complicated network of money transfers when they discovered money shifting from Kingfisher's accounts to Mallya's offshore firms. Mallya fled India, and he is currently being extradited to face accusations. The case resulted in stricter guidelines for bank loan approvals and highlighted the value of forensic accounting in detecting international financial wrongdoing[7].

In *Yes Bank Fraud Case* (2020): One of the top private banks in India, Yes Bank, came under fire after its founder, Rana Kapoor, was charged with giving high-risk loans to questionable businesses in return for bribes. Shareholders and depositors suffered significant losses as a result of the bank's failure. After tracking down the fraudulent loans and examining questionable money transactions, forensic investigators discovered a network of bribery-channelling shell corporations. Finding Kapoor's involvement in the scam required a combination of financial analysis, anomaly identification, and document scrutiny. The episode resulted in tighter regulation of corporate lending practices in private banks after the Reserve Bank of India stepped in to save Yes Bank. The case also demonstrated how important forensic accounting is in preventing insider fraud in the banking sector[8].

These examples have not only shown how well forensic accounting works to identify and look into intricate financial scams, but they have also highlighted how important it is to keep improving the fraud prevention systems in India's financial system. They have spearheaded regulatory changes and reaffirmed the value of accountability, openness, and sophisticated forensics in preserving public confidence.

[4] *M/S. Satyam Computer Services Limited, v Directorate of Enforcement*, W.P.No.37487 of 2012 & WAMP.

[5] *Punjab National Bank v Nct of Delhi & Anr.* CRL.M.C. 2696/2019.

[6] *Union Of India v Infrastructure Leasing and Financial*, Company Appeal (AT) No. 346 of 2018.

[7] *Kingfisher Airlines Ltd v Union of India and Ors*, WRIT PETITION (L) NO. 1684 OF 2015.

[8] *Rana Kapoor v Directorate of Enforcement*, CRIMINAL BAIL APPLICATION NO (ST). 4999 OF 2020.

8. Techniques And Tools Used In Forensic Accounting

A variety of strategies are used in forensic accounting, ranging from sophisticated digital forensics to more conventional approaches like financial statement analysis and auditing. Forensic accountants in India analyze vast amounts of financial data, spot questionable transactions, and spot fraud trends using sophisticated software programs like IDEA, ACL, and EnCase. Artificial Intelligence (AI) and forensic data analytics are also becoming more and more common, which helps accountants identify intricate schemes more quickly. A range of methods and resources are used in forensic accounting to assist experts in identifying, looking into, and stopping financial wrongdoing. These techniques combine cutting-edge technology, investigative abilities, and conventional accounting procedures to find anomalies and fraudulent activity.[9]

9. Challenges in Forensic Accounting in India

The forensic accounting sector in India has both opportunities and difficulties. Rapid technological advancements and the growth of complex financial operations have raised the demand for specialized knowledge and abilities. Nonetheless, limited awareness, inadequate infrastructure, and the need for ongoing professional development are barriers to the growth of forensic accounting in the country. Forensic accounting is crucial in India for detecting and preventing financial fraud and misconduct, safeguarding the interests of businesses, investors, and the whole economy. Forensic accountants can detect fraudulent conduct, locate assets, calculate damages, and provide testimony in court by applying their specific knowledge.

1. Regulatory Limitations and Enforcement Issues

Despite advancements in forensic accounting, regulatory enforcement remains a challenge in India. Many cases are delayed due to bureaucratic processes, and legal ambiguities can hinder timely prosecution. The country lacks a comprehensive legal framework that mandates forensic audits in cases of suspected fraud, which can limit the scope of investigations.

2. Limited Resources and Expertise

The demand for skilled forensic accountants exceeds supply in India. Many professionals lack formal training in forensic accounting, and some organizations are reluctant to invest in the necessary resources. Additionally, forensic accountants face challenges related to accessing data, especially in cases involving cross-border transactions.

3. Resistance from Organizations and Lack of Transparency

Companies in India may hesitate to disclose fraud due to reputational concerns. There is often resistance to forensic audits, which can hamper investigations. Forensic accountants may also face difficulties obtaining full cooperation from all parties involved, affecting the depth of their analyses.

4. Technological Challenges and Emerging Threats

The digitization of financial institutions has led to an increase in frauds involving cyberspace. To handle new risks like ransomware attacks and cryptocurrency-related fraud, forensic accountants need to be up to date on their abilities. Effective investigations may be hampered by a lack of access to sophisticated tools and cyber knowledge.

[9] Manas, C., 'Problems and prospects of forensic accounting profession in India' (2014) International Journal of Informative and Futuristic Research, 2(1), 1-9.

10. Recent Developments In Forensic Accounting In India

To improve forensic accounting procedures, the Indian government has taken action. Stricter compliance standards, like requiring forensic audits for businesses implicated in significant financial wrongdoing, are among the initiatives. To increase proficiency and elevate professional standards, the Institute of Chartered Accountants of India (ICAI) also provides certification programs in forensic accounting. Due to a rise in financial fraud instances, legislative changes, and increased awareness of corporate governance, forensic accounting in India has advanced significantly in recent years.

Some key developments include:

1. Enhanced Regulatory Focus

In India, regulatory bodies like the Securities and Exchange Board of India (SEBI), the Reserve Bank of India (RBI), and the Ministry of Corporate Affairs (MCA) have become more stringent about fraud detection and reporting. SEBI, for instance, has mandated forensic audits for companies under investigation for suspicious activities. This has increased the demand for forensic accounting expertise in corporate governance and financial reporting.

2. Introduction of Forensic Audit Standards

The Institute of Chartered Accountants of India (ICAI) introduced the Forensic Accounting and Investigation Standards (FAIS) in 2020, a comprehensive framework for conducting forensic audits. These standards provide clear guidelines for forensic accountants, fostering consistency, quality, and transparency in investigations.

3. Digital Forensic Capabilities

The rise of digital transactions and e-commerce has led to advancements in digital forensic tools and techniques in India. Forensic accountants increasingly use advanced data analytics, artificial intelligence (AI), and machine learning to identify anomalies, patterns, and red flags in vast datasets. This technology- driven approach enables faster and more accurate detection of financial irregularities.

4. Government initiatives against Financial Crimes

The Indian government has introduced several measures to counter financial crimes, such as demonetization, the Goods and Services Tax (GST), and the implementation of the Insolvency and Bankruptcy Code (IBC). These policies have indirectly fueled the need for forensic accounting to uncover tax fraud, money laundering, and insolvency-related misconduct.

5. Corporate Demand for Forensic Services

As a preventative step, many Indian corporations are investing in strong forensic accounting procedures in response to mounting demands for openness. In addition to fortifying internal controls, this proactive strategy aids businesses in becoming more resilient to financial crime.

6. Expanding Role in Litigation Support

In India, forensic accountants are increasingly involved in court proceedings about intellectual property, financial disputes, and other types of business litigation. They aid courts and arbitrators in comprehending complex financial data by offering expert testimony and supporting documentation.

These changes highlight how crucial forensic accounting is to India's changing financial environment. Forensic accounting will probably become more and more important in the fight against financial crime and in fostering confidence in India's financial institutions as the nation continues to adopt international norms and technologies.

Conclusion

In India, forensic accounting has been essential for identifying, looking into, and stopping financial wrongdoing. Cases like Satyam, Nirav Modi, and IL&FS demonstrate how important forensic accountants are in identifying intricate frauds and bringing offenders to justice. Regulatory restrictions, a lack of experience, and changing fraud tactics present difficulties for forensic accounting despite its tremendous achievements. India's financial integrity can be improved and fraud risks reduced by enhancing regulatory frameworks, encouraging openness, and fortifying forensic accounting procedures. To identify, look into, and stop financial misconduct, forensic accounting is crucial. Forensic accountants offer crucial insights that promote accountability, openness, and trust in financial institutions by combining their understanding of legal frameworks, investigation techniques, and accounting expertise. Their capacity to analyze intricate financial data and reveal hidden anomalies aids businesses in spotting fraudulent activity and putting in place more robust internal controls to stop wrongdoing in the future. Forensic accounting will continue to play a larger role as financial fraud gets more complex, strengthening the integrity of financial practices globally and acting as a vital defence against financial crimes.

References

- Alabdullah, T. T. Y., Alfadhl, M. M. A., Yahya, S., & Rabi, A. M. A. (2014). The role of forensic accounting in reducing financial corruption: A study in Iraq. International Journal of Business and Management, 9(1), 26.
- Ehioghiren, E. E., & Atu, O. O. K. (2016). Forensic accounting and fraud management: Evidence from Nigeria. Igbinedion University Journal of Accounting, 2(8), 245-308.
- Eko, E. U., Adebisi, A. W., & Moses, E. J. (2020). Evaluation of forensic accounting techniques in fraud prevention/detection in the banking sector in Nigeria. International journal of finance and accounting, 9(3), 56-66.
- Bhasin Madan, "Forensic Accounting: A New Paradigm for Niche Consulting." Journal of Chartered Accountant 200 P.No.1000-1010 ISSN 2349-7807
- Deepak Kumar Mandal, "The Role Of Forensic Accounting In Detecting & Preventing FraudInSelected Indian Companies", <https://shodhgangotri.inflibnet.ac.in/bitstream/20.500.14146/12441/1/deepak%20kumar%20mandal%202021.pdf>.
- Kanchan, 'The Role of Forensic Accounting in Fraud Investigation', (2021) IJRBS 2455-2992 <https://www.ijrbs.com/wp-content/uploads/2021/12/Kanchan.pdf> .

DIGITAL EVIDENCE

Shreya Shukla
Student, United University, Prayagraj

ABSTRACT

Digital evidence has become a cornerstone in modern legal proceedings, playing a critical role in criminal, civil, and regulatory cases. Derived from electronic devices, digital evidence includes emails, chat logs, social media posts, metadata, and multimedia files. While offering substantial benefits in proving or disproving claims, its admissibility faces challenges such as authentication, chain of custody, and jurisdictional issues. The increasing prevalence of encryption, anonymization, and cyber manipulation like deepfakes further complicate its reliability. This paper explores the types, sources, and legal considerations surrounding digital evidence, and the technological challenges affecting its integrity. It emphasizes the need for harmonized legal frameworks, advancements in digital forensics, and training for legal professionals to utilize digital evidence effectively. By addressing these challenges, this research contributes to the broader discourse on strengthening justice systems in the digital age.

Key words: *Digital evidence, legal admissibility, authentication, chain of custody, cyber security, digital forensics, encryption, deep fakes, jurisdiction*

Introduction

With rapid digitalization, the legal landscape has evolved to accommodate digital evidence, which includes emails, text messages, social media posts, and metadata. Courts worldwide now rely on digital evidence in both civil and criminal cases, necessitating stringent legal frameworks to ensure its authenticity and admissibility. However, digital evidence poses significant challenges related to its collection, preservation, and presentation in court. This paper discusses the fundamentals of digital evidence, the laws governing it, its challenges, and best practices for its use in judicial proceedings.

1. What Is Digital Evidence?

The evidence is generally termed as proof of records or any relevant information explanation to Section 79A of the Information Technology Amendment Act 2008 defines electronic evidence as any information with values that is stored or transmitted electronically, and it includes evidence such as computer data, digital audio digital videos cell phones and digital fax machines. Digital evidence refers to stored transmitted or collected information that is used as proof before the court of justice than formation is stored transmitted or collected in digital media like computers mobiles and other electronic devices digital evidence may be in numeral forms including messages pictures videos or any other digital forms there is a no need for hand it and notes for the fingerprint test during an investigation about digital evidence it is always stored in an electronic form not in a traditional paper document.

The scope of digital evidence plays a major role in different areas including legal proceedings, cyber security, corporate investigation, e-discovery, intellectual property theft, forensic analysis, and many other areas it is in many forms including electronic communication, digital documents, etc.

2. Need for Digital Evidence in the Modern Legal System

Digital evidence has become a critical component of modern legal proceedings due to the increasing reliance on digital technology in personal, professional, and criminal activities. The need for digital evidence arises from several factors, including the rise in cybercrimes, online transactions, and the use of digital communication in both criminal and civil matters.

1. Growing Dependence on Digital Technology: With the widespread use of computers, mobile phones, social media, and cloud storage, significant amounts of information are stored and transmitted digitally. This data can

serve as crucial evidence in various legal cases.

2. Proliferation of Cyber Crimes: Hacking, identity theft, financial fraud, cyberstalking, and data breaches require digital forensic analysis to track perpetrators and gather admissible evidence.

3. Digital Communication as Evidence: Emails, text messages, and social media posts: Used in cases involving defamation, harassment, business disputes, and fraud. Call logs and GPS data: Help establish the location and movements of individuals in criminal cases.

4. Role in Financial and Corporate Crimes: Electronic records and audit trails are essential in white-collar crimes like embezzlement, tax fraud, and money laundering. Blockchain and cryptocurrency transactions are increasingly used to investigate illicit financial activities.

5. Enhancing Accuracy and Reliability: Unlike traditional physical evidence, digital evidence often provides precise timestamps, metadata, and access logs, helping establish timelines and accountability.

6. Use in Civil Litigation and Family Law Digital contracts and agreements: Evidence in contract disputes. Social media and emails: Used in divorce, custody battles, and defamation cases.

7. Law Enforcement and National Security: Governments and law enforcement agencies use digital evidence to track terrorism, cyber threats, and organized crime. Surveillance footage, intercepted communications, and data analytics play a crucial role in such investigations.

8. Challenges and Legal Considerations:

- Authentication and admissibility: Ensuring digital evidence is not tampered with and meets legal standards.
- Privacy concerns: Balancing evidence collection with individual rights and data protection laws.
- Jurisdiction issues Cyber Crimes often involve multiple countries, making legal proceedings complex.

3. Types of Digital Evidence

1. Computer and File-Based Evidence: This includes data stored on computers, external hard drives, USB devices, or cloud storage that can be used as evidence in legal proceedings.

a) Files and Documents:

- Text files (e.g.,.docx,.pdf,.txt) – Can contain incriminating information, contracts, or confidential data.
- Spreadsheets (e.g., .xls, .csv) – Often used in financial crimes and fraud investigations.
- Deleted or modified files – Recovering deleted files can provide crucial insights into criminal activities.

b) Metadata: Provides details about file creation, modification, and access and it helps in verifying the authenticity of documents and detecting forgery.

2. Internet-Based Evidence: This type of evidence is obtained from online sources such as websites, emails, and cloud storage.

a) Emails:-

- Used in fraud cases, corporate disputes, and cybercrimes.
- Email headers provide IP addresses, timestamps, and recipient details for tracking.

b) Web History and Cache: Websites visited, downloads, and search queries can establish intent and past activities. It is useful in cyberstalking, fraud, and hacking investigations.

c) Cloud Storage Data:

- Documents stored in Google Drive, Dropbox, OneDrive, etc.
- Challenges include encryption and jurisdictional issues for accessing data.

3. Social Media and Messaging Evidence: Social media platforms (Facebook, Twitter, Instagram, WhatsApp, Telegram, etc.) contain vast amounts of evidence.

a) Posts, Comments, and Messages

- Social media content is used in cases of defamation, harassment, cyberbullying, and criminal investigations.

- Private messages and group chats can reveal crucial conversations in legal disputes.

b) Photos and Videos

- Geotagging (location data) in photos helps track the whereabouts of individuals.
- Deep fakes detection and image analysis are used to verify authenticity.

4. Mobile Device Evidence: Mobile phones contain various forms of digital evidence, making them crucial in investigations.

a) Call Logs and SMS

- Call records help establish communication patterns between suspects.
- Deleted SMS messages can sometimes be recovered and used in legal cases.

b) GPS and Location Data

- Location tracking from GPS apps, maps, and ride-hailing services can establish alibis or criminal presence at a crime scene.

c) Installed Apps and Data

- Banking apps, encrypted messaging apps, and social media can reveal financial transactions, secret conversations, or illicit activities.

5. Audio and Video Evidence:- Multimedia files often play a significant role in proving or disproving claims in legal cases.

a) Recorded Phone Calls and Voicemails

- Used in cases involving threats, blackmail, and business disputes.

b) Surveillance Footage (CCTV, Dash Cams, Bodycams)

- Used in criminal investigations, car accidents, and fraud detection.

c) Digital Forensics on Edited Media

- Deepfake videos and doctored audio can mislead investigations, requiring forensic analysis to confirm authenticity.

6. Network and Log-Based Evidence: This includes data captured from networks and logs that help in cybercrime investigations.

a) IP Addresses and Network Traffic

- Identifies the source of cyberattacks, hacking attempts, and unauthorized access.

b) Firewall and Server Logs

- Tracks suspicious activities in organizations or government systems.

c) Intrusion Detection System (IDS) Log: Used to identify and prevent cyber threats.

7. Cryptocurrency and Financial Digital Evidence: As digital currencies become popular, they are increasingly involved in financial crimes.

a) Blockchain Transactions: Bitcoin and other cryptocurrency transaction records can be traced using blockchain analysis.

b) Digital Wallets and Exchange Records: Investigators track money laundering, fraud, and illegal transactions through digital wallets.

8. Internet of Things (IoT) and Smart Device Evidence: With smart home devices, new sources of digital evidence are emerging.

a) Smart Home Assistants (e.g., Alexa, Google Assistant): Voice recordings may be used as evidence in criminal cases.

b) Smart Cameras and Doorbell Footage: Helps in burglary and trespassing cases.

c) Wearable Devices (Smartwatches, Fitness Trackers): Heart rate, movement patterns, and GPS data provide alibi verification.

4. Admissibility Of Digital Evidence In Indian Law

In India, the admissibility of digital evidence depends on the different laws, and the legal ruling of the Indian legal system has given legal recognition to digital evidence and such recognition of digital evidence is covered under different laws that include as following:-

● **Indian Evidence Act 1872**:- Before the enactment of the Information Technology Act, of 2000, the Indian Evidence Act, of 1872 (IEA) did not explicitly recognize electronic records. However, after the 2000 amendment, key provisions were introduced under Sections 65A and 65B to regulate the admissibility of electronic evidence.

A. Section 65A & 65B – Special Provisions for Electronic Evidence
Section 65A states that electronic evidence shall be proved following Section 65B
Section 65B (1) & (2) lay down conditions for admissibility:

- The electronic record must be produced by a lawfully operating computer in regular use.
- The computer must have been functioning properly during the relevant time.
- The record should have been regularly fed into the system as part of normal business activity.

Section 65B (4) mandates a certificate of authenticity, signed by a person in charge of the computer system, to validate the electronic record.

5. Judicial Interpretation

- State (NCT of Delhi) v. Navjot Sandhu (2005) The Supreme Court initially held that electronic records could be admissible even without compliance with Section 65B(4)[1].

- Anvar P.V. v. P.K. Basheer (2014) – This decision overruled Navjot Sandhu and emphasized that compliance with Section 65B is mandatory for the admissibility of electronic evidence[2].

- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) – Reaffirmed that a Section 65B certificate is essential, and an alternative method cannot substitute it unless the original device is produced[3].

Bhartiya Sakshya Bill, 2023: The Bhartiya Sakshya Bill, 2023, aims to replace the Indian Evidence Act, of 1872 and incorporates modern provisions for digital evidence.

Key Provisions Related to Digital Evidence:-

1. Section 61 (equivalent to Section 65A of the IEA) – States that the proof of electronic records must comply with special provisions.

2. Section 62 (similar to Section 65B of the IEA) – Mandates compliance with strict conditions, including the requirement of an authenticity certificate.

3. Introduction of AI-Based & Blockchain Evidence – Recognizes modern technological advancements such as AI-generated records and blockchain-based transactions.

6. Impact on Digital Evidence

- Expands the scope of admissibility by aligning Indian law with global digital forensic practices.
- Removes ambiguities surrounding cloud-stored data and third-party servers.

Information Technology Act, 2000: The Information Technology Act, 2000 (IT Act) plays a crucial role in defining legal recognition and admissibility of digital evidence.

- Section 4 – Grants legal recognition to electronic records.
- Section 5 – Validates electronic signatures as equivalent to handwritten signatures.
- Section 65 – Defines penalties for tampering with electronic records, ensuring their integrity.
- Section 67A – Regulates the admissibility of electronic contracts and communications.

The Banker's Books Evidence Act, 1891:- The Bankers' Books Evidence Act, of 1891, allows banks to produce electronic records as evidence in court. Section 2(3) – Defines “bankers' books” to include ledgers, day books, account books, and electronic records.

Section 2A – Recognizes the evidentiary value of printouts and copies of bank records stored in electronic form.

Section 4 – Exempts banks from producing original physical records if authenticated digital copies are presented.

7. Impact on Financial Digital Evidence

- Enables courts to rely on electronic bank statements as primary evidence.
- Reduces fraud by ensuring legal acceptance of digital banking records.

[1] State (NCT)of Delhi vs. Navjot Sandhu (2005) 11 SCC 600

[2] Anvar P.V.vs P.K. Basheer , (2014) 10 SCC 473

[3] Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal (2020) 7 SCC 1

8. Convention Related to Digital Evidence

Several international conventions and frameworks address digital evidence, focusing on its admissibility, collection, and use in legal proceedings. The most significant among them is the Budapest Convention on Cybercrime (2001). Below is a detailed breakdown of this and other conventions related to digital evidence:-

1. Budapest Convention on Cybercrime (2001)

Overview: - The Convention on Cybercrime, also known as the Budapest Convention, was adopted by the Council of Europe (CoE) in 2001. It is the first international treaty addressing cybercrime and digital evidence.

Key Provisions Related to Digital Evidence:

Procedural Measures (Chapter II, Section 2):

- Expedited preservation of stored computer data (Article 16): Authorities can order service providers to preserve data to prevent tampering.
- Expedited preservation and partial disclosure of traffic data (Article 17): Enables quick preservation of traffic data for further investigation.
- Production Order (Article 18): Authorities can require individuals or entities to produce digital evidence.
- Search and Seizure of Stored Computer Data (Article 19): Defines rules for legal searches of digital storage devices.
- Real-time Collection of Traffic Data (Article 20): Allows authorities to collect data on communications (metadata).
- Interception of Content Data (Article 21): Enables lawful interception of communication content.

International Cooperation (Chapter III): Countries must assist each other in collecting and exchanging digital evidence and mutual legal assistance (MLA) is required for cross-border digital investigations.

Importance of the Budapest Convention:

1. Sets a global standard for digital evidence handling.
2. Promotes international cooperation in investigating cybercrime.
3. Enhances legal frameworks for digital forensic investigations.

Challenges

- Some countries, including Russia and China, oppose it, arguing that it gives excessive control to Western nations.
- Developing nations may struggle with implementation due to technological and legal gaps.

2. Malabo Convention (2014) – African Union Convention on Cyber Security and Personal Data Protection:-

Overview: The Malabo Convention, adopted by the African Union (AU), focuses on cybercrime, cyber security, and data protection.

Provisions Related to Digital Evidence:

- Promotes the harmonization of digital evidence laws in African nations.
- Requires judicial and law enforcement authorities to develop capabilities for handling digital evidence.
- Encourages regional and international cooperation in investigating cybercrimes.

Challenges:

- Low ratification rate: Many AU member states have not ratified or implemented the convention.

- Limited enforcement mechanisms due to varying legal systems.

3. United Nations Cybercrime Treaty (Under Negotiation)

Overview: The United Nations (UN) is drafting a cybercrime convention to create a global framework for combating cybercrime and handling digital evidence. It is expected to supplement the Budapest Convention and create a universally accepted standard.

Proposed Provisions Related to Digital Evidence:

- International legal cooperation in cyber investigations.
- Harmonization of national laws for handling digital evidence.
- Protection of human rights while investigating digital crimes.

Current Status: It is still under negotiation and expected to address the concerns of countries that are not part of the Budapest Convention.

4. The e-Evidence Regulation (European Union)

Overview: The EU e-Evidence Regulation, adopted in 2023, aims to streamline the process of obtaining digital evidence across EU member states.

Key Features:

- Allows law enforcement to directly request electronic evidence from service providers in another EU country.
- Requires companies like Google, Meta, and Microsoft to comply with evidence requests within ten days (or six hours in urgent cases).

Significance:

1. Reduces delays in cross-border digital investigations.
2. Strengthens legal frameworks for handling digital evidence in criminal cases.

9. Role of Digital Evidence in Cybercrime Investigation: - Digital evidence plays a pivotal role in cybercrime investigations as it provides concrete proof of criminal activities committed using digital devices and online platforms. Cybercrimes such as hacking, identity theft, phishing, cyberstalking, and ransomware attacks are largely investigated through digital footprints left by perpetrators. Investigators analyze logs, metadata, IP addresses, encrypted data, and digital communications to trace and prosecute offenders. The role of digital evidence in cybercrime investigations includes:

1. Tracing Cybercriminals: Digital forensics helps identify perpetrators by analyzing IP logs, network traffic, and digital signatures.

2. Corroborating Evidence: It supports other forms of evidence like witness testimony and physical records.

3. Reconstructing Crime Scenes: Investigators use digital artefacts such as timestamps, deleted files, and system logs to recreate a cyber-attack timeline.

4. Identifying Malware and Attack Methods: Analyzing malicious software and exploits used by criminals aids in understanding the attack mechanism.

5. Ensuring Convictions: Strong digital evidence reduces ambiguities and strengthens legal arguments in court.

10. Significance of Digital Evidence in Protecting Intellectual Property Rights (IPR): Digital evidence is crucial in IPR cases as intellectual property theft, counterfeiting, and copyright violations are increasingly committed online. Some key aspects of its role include:

1. Identifying Unauthorized Use: Digital evidence helps track instances of copyright infringement, trademark violations, and software piracy.

2. Proving Ownership and Authorship: Metadata in digital files, blockchain records, and timestamps establish rightful ownership of content.

3. Tracking Distribution Channels: Forensic tools help identify unauthorized distribution and reproduction of copyrighted materials.

4. Preventing Trade Secret Theft: Digital forensics is used to detect insider threats and unauthorized data transfers in corporate environments.

5. Legal Action and Compensation: Courts rely on digital evidence to determine damages and grant injunctive relief in IPR disputes.

11. Importance of Digital Evidence in Forensic Investigation: - Digital evidence is integral to modern forensic investigations as it helps establish facts, links suspect to crimes and provide detailed insights into criminal activities. Its importance includes:

1. Preserving Digital Trails: Every digital action leaves a footprint, which forensic experts can use to trace criminal behaviour.

2. Enhancing Criminal Profiling: Analyzing an individual's digital activity can help in understanding their intentions and potential involvement in crimes.

3. Supporting Cross-Examination: Digital records like emails, chat logs, and financial transactions provide concrete proof in legal proceedings.

4. Providing Timelines: Time-stamped logs, messages, and access records help establish the sequence of events in a case.

5. Assisting in Corporate Investigations: Digital forensics is essential in investigating fraud, embezzlement, and insider trading cases.

12. Major Types of Digital Forensics: - Digital forensics is broadly categorized into various fields based on the nature of the evidence being analyzed:

1. Computer Forensics: Deals with the recovery and analysis of data from computers, hard drives, and storage devices.

2. Network Forensics: Focuses on monitoring and analyzing network traffic to detect cyberattacks and data breaches.

3. Mobile Forensics: Involves retrieving data from mobile devices, including call logs, messages, and app usage.

4. Database Forensics: Examines databases for unauthorized access, data tampering, or fraudulent transactions.

5. Cloud Forensics: Investigates crimes involving cloud storage and online service platforms.

6. Malware Forensics: Identifies and analyzes malicious software, such as viruses, Trojans, and ransomware.

7. IoT Forensics: Deals with digital evidence from smart devices, such as security cameras and smart home assistants.

13. Judicial Pronouncements Surrounding Digital Evidence: - Several landmark judicial decisions have shaped the admissibility and use of digital evidence:

1. Anvar P.V. v. P.K. Basheer (2014) – The Supreme Court of India ruled that digital evidence must comply with Section 65B of the Indian Evidence Act for admissibility.

2. Tomaso Bruno & Anr v. State of Uttar Pradesh (2015) – The Supreme Court recognized CCTV footage as crucial digital evidence in criminal cases.

3. Shafhi Mohammad v. State of Himachal Pradesh (2018) – Relaxed the strict procedural requirements of Section 65B certification when primary evidence was available.

4. State v. Navjot Sandhu (Parliament Attack Case, 2005) – The court admitted digital evidence, including call records, as key evidence in a terrorism trial.

14. Benefits of Digital Evidence in Legal Proceedings:-

1. Strong Evidentiary Value: Digital evidence provides precise and objective data that is difficult to manipulate.

2. Faster Investigations: Automated tools expedite the process of analyzing digital data.

3. Remote Access & Storage: Cloud-based evidence can be retrieved from anywhere without physical constraints.

4. Cross-Border Collaboration: Digital evidence facilitates international cooperation in cybercrime investigations.

5. Enhances Fair Trial: Clear and indisputable digital records ensure that justice is served effectively.

15. Challenges in Handling Digital Evidence in India:-

1. Authentication Issues: Ensuring the integrity and originality of digital evidence is challenging.

2. Section 65B Compliance: Admissibility of electronic evidence is often hindered by procedural requirements.

3. Lack of Skilled Personnel: Digital forensics expertise is still limited in many law enforcement agencies.

4. Tampering & Spoofing: Digital evidence can be altered or fabricated, requiring robust verification mechanisms.

5. Jurisdictional Challenges: Cross-border cybercrimes create legal complications in evidence collection and prosecution.

6. Encryption & Privacy Laws: Strong encryption technologies and data protection laws sometimes obstruct investigations.

16. Different Global Positions on the Admissibility of Digital Evidence: - Different countries have varied legal frameworks for the admissibility of digital evidence:

1. United States: Governed by the Federal Rules of Evidence, digital evidence must be authenticated and comply with hearsay exceptions.

2. United Kingdom: Digital evidence is admissible under the Police and Criminal Evidence Act (PACE) 1984, provided its integrity is maintained.

3. European Union: The General Data Protection Regulation (GDPR) impacts how digital evidence is collected and used in trials.

4. China: Has stringent cyber laws and requires state verification of digital evidence before admitting it in court.

5. Australia: The Evidence Act 1995 allows digital evidence if its authenticity and reliability are established.

17. Admissibility of Digital Evidence in International Criminal Courts: - International criminal courts, such as the International Criminal Court (ICC) and International Criminal Tribunals, rely on digital evidence for prosecuting war crimes, genocide, and crimes against humanity. Key considerations include:

1. Authentication: Digital evidence must be verified through forensic methods to ensure credibility.

2. Chain of Custody: Proper documentation of how digital evidence is collected, stored, and analyzed is essential.

3. Hearsay & Reliability: Courts examine metadata, timestamps, and sources to determine reliability.

4. Use in War Crime Investigations: Digital evidence, such as satellite images, intercepted communications, and social media data, is increasingly used in international trials.

5. Challenges: Issues like deep fakes, manipulated media, and jurisdictional limitations complicate the acceptance of digital evidence in international courts.

Conclusion

Digital evidence has become an indispensable component of modern legal systems, playing a crucial role in cybercrime investigations, intellectual property protection, forensic analysis, and international criminal trials. Its ability to provide concrete, time-stamped, and verifiable records strengthens legal proceedings, ensuring accurate fact-finding and fair justice. However, challenges such as authentication issues, admissibility standards, jurisdictional conflicts, and data tampering require robust legal frameworks and advanced forensic techniques. To maximize the effectiveness of digital evidence, courts and law enforcement agencies must adopt standardized procedures, invest in forensic expertise, and ensure compliance with evolving legal norms. Strengthening international cooperation and harmonizing digital evidence laws across jurisdictions will further enhance its reliability and usability. As technology continues to evolve, adapting legal mechanisms to effectively handle digital evidence will be essential in maintaining the integrity and efficiency of judicial processes.

EXPLORING THE RIGHT TO BE FOR GOTTEN : STATUTORY RECOGNITION AND CHALLENGES

Shaurya Pratap Singh
B.A LL.B. (H) student, The ICFAI University, Dehradun

Gaurav Kumar
B.A LL.B. (H) student, The ICFAI University, Dehradun

ABSTRACT

In the digital era, where data persistence is crucial, the Right to Be Forgotten (RTBF) emerges as a significant legal development. It refers to the ability of individuals to erase, limit, delink, delete, or correct personal information on the Internet that is misleading, embarrassing, or irrelevant. This right finds its spotlight in the case of Google Spain, embodied in the European Union's General Data Protection Regulation (GDPR). The US, much advanced in technology still has no cover. In India, the Digital Personal Data Protection Act, 2023, Section 12, carries implications without direct references to the RTBF, its enforcement aspects are still in development. The given landmark points in the Indian High Courts have raised issues on the essentiality and challenges of RTBF regarding privacy violations, breache storeputations, and protection of the victims, potential censorship implications, and rewriting history, through the prism of technological logistics such as data retention as well as erasure mechanisms. This paper explores the background of the RTBF, its legal recognition in the EU and India, key judicial precedents set by Indian courts, implicit in corporation in the DPDP Act 2023 potential technological and legal challenges, and its negative side.

Key words: *Right to be forgotten, Google Spain Case, DPDP Act, GDPR, Judicial cases.*

Introduction

In today's world, under the real mof social media, an individual presence is evaluated on how much they are active on social media. Various search engines like Google,Yahoo, and Firefox, etc. are synonyms of search and different social media platforms like Facebook, Instagram, and WhatsApp are other examples that certify that people using it are alive in this virtual world. Indeed, in the present scenario, this virtual world decides the credibility of an individual.

The Internet connects one corner of the world to another. The advancement of internet communication has made things easier and turned this world into a global village. There are currently4.95 billion active Internet users worldwide, and 65.6 percent of the entire world's population has the Internet, there are 4.28 billion unique mobile Internet users, and there are over 1.8 billion websites on the World Wide Web[1]. Thus, ourwall of privacy is becoming

thinner day by day and making our data vulnerable to the public often. Just imagine how we enjoy others' controversies on the internet but how it will feel when our data or we can say our most awkward data is made open to all the sources, humiliating, right!

A person's personal information is no longer limited to government files and documents in the age of Google, Facebook, Twitter, and other social media sites. People are now just a search away, and their information is easily accessible on the internet. This dramatic shift in the type and scope of personal information on the internet is a major issue. To appear because of a Google search, you do not need to be an overachiever or have committed a criminal offense.

Backgroundof theRight to be Forgotten

The French legal system established the jurisprudence of the 'Right to be Forgotten' in 2010, also known as Droit

[1] 10InternetStatisticsEveryMarketerShouldKnowin2024availableat:https://www.oberlo.com/blog/internet-statistics(last visited on November 29, 2024).

a l'oubli. The Right to be Forgotten helped ex-convicts by erasing the record of their crimes and criminal past once they served their sentence. In1998,MarioCosteja González, a Spaniard, faced financial troubles and needed money urgently. Consequently, he placed a property up for auction in the newspaper, and the advertisement happened to make its way onto the internet by chance. Regrettably, the internet did not forget Mr. Gonz´. News of the sale was still findable on Google after he sorted out his financial trouble, leading people to believe he was still bankrupt. Naturally, this led to significant harm to his reputation, causing him to bring the issue to court. In the end, this case led to the creation of the idea of the 'Right to be forgotten[2].

Another case related to the issue of the right to be forgotten was in Argentina, though the idea of the right to be forgotten was not popular when this case was decided, where a musician and pop star named Virginia da Cunha, objected to the results that came up when people googled her and brought a case against the search engine Google for damaging her reputation because her name was linked with pornography and prostitution .The court's primary decision came in da Cunha's favour in 2009, ordering Google and Yahoo to remove her name's suggestion from pornography and prostitution. Later in August 2010, an appeal court reversed the primary decision, finding that the searchengines were not liable under general rules of tortliability and favoured Google and Yahoo. In 2014, the Supreme Court of Argentina ruled in favour of search engines. This judgement raised a fundamental question related to the free exchange of ideas and information on the Internet, as well as the need to protect individuals from harm caused by online publications.

In 2014, the European Court of Justice decided the case that involved the issue of the right to be forgotten. The fact of the case was that there was a man named Mario Costeja González, a Spanish, who had run into financial difficulties and was in desperate need of money in 1998. As a result, he advertised a property for auction in the newspaper, which by chance ended up on the internet. Unfortunately, Mr. González was not forgotten by the internet. As a result, news of the sale was searchable on Google long after he had resolved his financial problems, and everyone who looked him up assumed he was bankrupt. Understandably, this caused significantdamagetohisreputation,promptinghimtofilealawsuit.Thiscaseultimatelygave rise to the concept of the "right to be forgotten.”

The top European court favored the man and said that Google must delete the inadequate, irrelevant, or no longer relevant data from its search results when any EU citizen requests it[3] The CJEU ruled that it has jurisdiction to hear the case, that search engines are data controllers, and that the right to be forgotten requires search engines to delete personal information that is "inadequate, irrelevant or no longer relevant, or excessive concerning the purposes of the processing. "The CJEU, on the other hand, ruled that the right to be forgotten should not apply to information of public interest.

The Court of Justice of the European Union recognized this right to be forgotten under the EU Data Protection Directive 2014. As per Directive 2014, search engine platforms are required to stop or destroy the personal data of an individual after the required time or years if it is of no relevance to public use. The decision set an example for the EU's ability to enforce CJEU's decision on American companies even if their server is based outside Europe. Since then, Google has received more than 2.5 million requests for the removal of information from Europe, and as claimed by Google, it has removed 43% of requests it has received.

In another case in France, Google was fined by French privacy watchdog CNIL in 2016 for refusing to delist sensitive data from internet search results globally upon request in what is called the right to be forgotten. But the European Union's top court favoured Google in its judgement, saying that European law applies to Google's European domain only.

[2] The Evolution of Right to be Forgotten in India” available at: https://www.scconline.com/blog/post/2022/01/27/the-evolution-of-right-to-be-forgotten-in-india/(lastvisitedon November 1, 2024)

[3] GoogleSpainSLandGoogle Inc v.AgenciaEspanola deProtectionDatosCaseC-131/12.

While the United States of America, the most advanced and powerful nation, does not have any statutes that talk about the right to be forgotten. However, New York State briefly introduced a bill that makes mandatory provisions for search engine store move in accurate, irrelevant, and excessive information about an individual. This bill identifies these data as of no use to the public, as there is a significant time lapse since the publication of these data. And these data are causing unwanted harm or defaming their reputation in business and day-to-day life.

The GDPR (General Data Protection Regulations)[4] will significantly strengthen the right to be forgotten in Europe. Article 17 of the GDPR establishes the Right to Erasure, which allows a data subject to request that a controller delete personal data about him or her without undue delay.

What the right to be forgotten means

The right to be forgotten is a right to remove publicly available personal information from online databases such as the internet, websites, blogs, searches, etc., or any other private link of information considering of right to privacy. This is also known as the right to erasure or the right to be delisted. The right has been recognized by the European Union's GDPR as a statutory right and upheld by many European courts and English courts.
The right to be forgotten is the right to have private information about a person removed from Internet searches and other directories under some circumstances.

Judicial pronouncement on the right to be forgotten

Before the enactment of DPDP Act, 2023, no law in India recognized the right to be forgotten. In India, the online search regime is mainly governed by the Information Technology Act of 2000. However, it does not empower citizens to ask the online search regime to delete their information. However, there are several cases in which various High Courts in India had recognized this right.

A case in which the right to be forgotten was recognized was The Karnataka High Court recognized the right to be forgotten in V. v. High Court of Karnataka[5]. Since the petitioner's daughter's name appeared in the cause title and could be easily found, it was intended to have her reputation damaged. The court ruled in the petitioner's favour and issued an order removing the name of the petitioner's daughter from the cause title and the orders. "This would be consistent with the trend in Western countries, where the 'right to be forgotten'is applied as a rule in sensitive cases concerning women in general, as well as particularly sensitive cases involving rape or harming the modesty and reputation of the individual concerned," the court concluded.

In Jorawar Singh Mundy v. Union of India[6], the Delhi High Court recognised the right to be forgotten. The High Court was hearing a plea of Jorawar Singh Mundy, an American citizen of Indian descent. He was charged under the narcotics case when he was on an India visit, but within a month of trial, he was acquitted and absolved from all charges by the trial court and Delhi High Court. After returning to the US, he studied law, and after a year he informed the Delhi High Court that every time he went for job interviews, potential employers ran a background check about him on Google; his name reflected on Google and other law-related websites of India. Thus, this reflection of his name on the website is a lack of employment for him. He requested the Delhi High Court to order Google, Lex. in, and the Indian Kanoon website to remove the judgement. Therefore, the Delhi High Court noted the irreparable harm that it may have done to Mundy's social life and career prospects, even though he was acquitted with in amonth he was charged, and gave him interim protection. The judgement was ordered to be removed from Google's search results, and India Kanoon was ordered to block the judgement from being accessed through search engines such as Google and Yahoo.

[4] GeneralDataProtectionRegulationRegulations (EU)2016/679

[5] (2017) SCC OnLineKar243.

[6] (2021) SCC OnLine Del2306

The High Court of Odisha in the case Subhranshu Rout @ Gugul vs State of Odisha[7], Upheld the right to be forgotten, as upheld by various high courts. This case deals with the objection able image of women being published online. The victim claimed to have been in love with the defendant for about a year before the incident. They both came from the same village and were classmates. One day, upon learning that her victim was alone in her home, the accused visited her and raped her. He also took photos and videos of the incident without her consent and started blackmailing her, giving life threats to her. The victim told her parents about these incidents, and in response, the accused uploaded her videos and photos on social media. Now due to this, her reputation was affected negatively. The High Court held that though there is a harsh punishment given in our statutes for offences of rape but, there is no mechanism for any individuals to remove objectionable photos from online content. The court ruled that in such circumstances, victims should be able to permanently remove their photos from the servers of social media platforms such as Facebook, as there is no law providing for this right. The court further ruled that the establishment of aprecedent of the right to be forgotten in India will play an important role in protecting the interests of women online.

Supreme Court, in its judgement of Justice K.S. Puttaswamy (Retd.) v. Union of India[8], held that the right to privacy and the right to be forgotten are fundamental rights and they are intrinsic parts of Article 21[9]. Privacy right is a natural right that exists permanently in all human beings.

Recently, a single-judge bench of Madras High Court, headed by Mr. Justice N. Anand Venkatesh, gave an order related to the right to be forgotten as a facet of the fundamental right to privacy. In the case before the single judge bench, the petitioner was seeking to remove his name from online content and a high court judgment order. Even though the petitioner was acquitted, they were named as an accused through out the preceding judgement. Therefore, the petitioner prayed for the removal of his name as it was depicting a negative image in society.

On the requests of the petitioner, the court ruled that the "right to be forgotten"cannot exist in the administration of justice, especially when it comes to court judgements.

Statutory recognition of the right to be forgotten in India

After the K.S. Puttaswamy case, the government decided to set up a committee under the chairmanship of Justice BN Srikrishna that submitted its report in July 2018 to the government along with the recommendation of its drafted Data Protection Bill. There port has a wide range of recommendations for strengthening privacy laws in India. Its proposals included restrictions on the processing and collection of data, a Data Protection Authority, the right to be forgotten, data localization, explicit consent requirements for sensitive personal data, etc. Some of the recommendations of the draft bill 2019 are: The bill regulates the processing of personal data of an individual (data principal)by a government and private entities (data fiduciaries). Processing is allowed only when an individual gives its consent to a private company, in a medical emergency, or by the state government for a benefits scheme.

- Data principal has the right to seek correction and access to their data from data fiduciaries.
- Data fiduciaries must notify data principals while processing their data as to its nature and purpose of data processing.
- Some exemptions are allowed in the interest of national security, integrity, or legal proceedings.
- Data must be stored within the territory of India.
- The draft bill recommends the establishment of a national-level Data Protection Authority (DPA).

[7] (2020)SCCOnLineOri878.

[8] (2017)10SCC1

[9] The ConstitutionofIndia,art.21.

- Any violation of the said provision of the bill, the data fiduciary will attract a fine of fifteen crore or 4% of annual turnover in case of violation in processing or transferring personal data. In the case of failure to conduct a data audit, the data fiduciary will be fined five crore or 2% of annual turnover, whichever is highest.

- Imprisonment of three years or a fine or both will be in the case of reprocessing of de- identified data without the consent of the data principal.

There are several issues related to the Indian data protection bill, as it does not give any specific common guidelines as to how the data fiduciaries will process the data fairly and reasonably and how they will be responsible. As there is no specific guideline mentioned in the bill, private entities and the government too can use this loophole for their benefit. Within this huge population, prevalent in digital illiteracy about data, personal information on online search platforms is also the main concern. The lack of proper digital infrastructure is also undermining the bill recommendation for data storage in India. It may hurt the start-up environment in the nation.

This data protection bill was referred to the Joint Parliamentary Committee for its recommendation in the bill. After several modifications, the Joint Parliamentary Committee tabled its report in December 2021 with eighty-one amendments and twelve recommendations. Several recommendations are:

a) The government may exempt any of its agencies from the bill.

b) The word' personal' ought to be dropped from the bill.

c) No social media platform would be allowed to operate in India unless its parent company, which controls the technology powering its services, sets up an office in the country.

However, in August 2022, the Union Government withdrew the bill. It stated that it would introduce a more comprehensive framework and contemporary privacy law as per the global standard to boost the digital economy. Later, in August 2023, the Indian Parliament enacted the Digital Personal Data Protection Act of 2023[10] (here in after, DPDP Act),but it has not been enforced yet.

The DPDP Act, 2023 does not recognise the right to be forgotten separately like it has been identified under the GDPR of the European Union, but it has been codified under section 12 of the Act, 2023. Data Principals whose data have been collected has been given several rights regarding their data. Section 12 is reproduced below:

'Section 12-Right to correction and erasure of personal data:

(1) A Data Principal shall have the right to correct, completion, update, and erase her data for the processing of which she has previously given consent. Including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(2) A Data Fiduciary shall upon receiving a request for correction, completion, or updating from a Data Principal:

a) Correct the inaccurate or misleading personal data;

b) Complete the incomplete personal data; and

c) Update the personal data

(3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for the erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data

[10] The Digital Personal Data Protection Act,2023 (Act22 of 2023)

unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.'

According to section 12 of the Act, 2023 Data Principal (whose data has been collected) has the right to correct, complete, erasure, and update his/her data subject to previous consent given by the Data Principal to the company. If the Data Principal requests a correction, completion, or update of their data, the Data Fiduciary, who processes the data must:

a) Correct inaccurate or misleading data.

b) Complete any incomplete data.

c) Update old or outdated data

d) Erase the data.

A Data Fiduciary can refuse to erase the data if it is required to retain it for a specific purpose (for ex: legal, compliance, or business-related purposes).

Section 12 of the Act, 2023 makes the Data Principals entitled to correct, complete, amend, or erase their data and at the same time puts a duty on Data Fiduciaries to do so unless they are bound by law to keep them. Thus, this section has given statutory recognition to the right to be forgotten under the Act of 2023.

In simple terms, in India, the government recognized the right to be forgotten in its enacted Personal Data Protection Act of 2023, but it has not been implemented yet and there is no specific law related to it till today. The Information Technology Act of 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which are the current legal framework, do not provide access to the right to be forgotten. This pull-out Act of 2023, however, aims to do so.

Recent Developments in RTBF: DPDP Rule Notification, January 2025

Recently, the Central Government notified DPDP Rule, 2025[11] which contains twenty-two rules and seven schedules to operationalize the DPDP Act 2023. Notification marked a significant milestone in India's effort to safeguard its citizens' data. India's commitment to creating a robust framework for protecting digital personal data. The regulations, which are straightforward to understand, are intended to empower citizens in the rapidly developing digital economy. In line with the DPDP Act, they aim to uphold the rights of citizens while strikingtheidealbalancebetweeninnovationandregulation,ensuringthateveryonemayprofit from India's expanding innovation ecosystem and digital economy. Additionally, they deal with issues including unauthorized commercial data use, digital damages, and breaches of personal data.

The draft rules place citizens at the core of data protection law, with key features like giving more control to citizens over their data, establishing clear responsibilities of data fiduciaries, the organization must obtain informed consent from data principals, ensuring transparency in data processing, and adopting robust security measures and complying with government guidelines. Further, Rules 2025 empowers individuals known as data principals by granting them rights like the right to access and correction of their data if they spot any inaccuracies. Right to erasure (also known as right to be forgotten) data principals can request the erasure of their data under specific conditions, like if the data is no longer necessary for its intended purpose or by withdrawing consent[12].

[11] DraftDigitalPersonalData Protection Rules,2025 available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2090271(last visited on January 20,2025)

[12] All you wanted to know about the Draft Digital Personal Data Protection Rules, 2025 available at: https://theleaflet.in/digital-rights/all-you-wanted-to-know-about-the-draft-digital-personal-data-protection-rules-2025(last visited on January 20, 2025)

Technological Challenges to the right to be forgotten

The idea of the Right to be Forgotten (RTBF) has gained popularity worldwide, especially considering the General Data Protection Regulation (GDPR) of the EU; however, India has distinct technological difficulties in implementing it.

Challenges arise in the intersection between generative artificial intelligence, especially large language models (LLM) such as ChatGPT, and the right to be forgotten (RTBF) creates unprecedented challenges. Their capacity to creating and process content presents serious obstacles to preserving private information and respecting the right to be forgotten. Due to their extensive use of sophisticated algorithms and vast volumes of data, these models have issues with deletion of information, erroneous content creation, and opaque operation. Three problems with LLM are:[13]

a) Data Persistence in LLMs: Generative AI models, when trained on large volumes of data, face difficulties in retroactively deleting personal information. Although techniques such as machine unlearning are under development, they do not yet guarantee a full and effective implementation of the right to be forgotten.

b) The problem of hallucinations: In addition to storing personal data, these models can generate erroneous or fictitious content. This capability poses an additional risk, as a 'hallucination' can involve sensitive information about individuals, generating serious legal and reputational implications.

c) Transparency and control: Both the GDPR and the Artificial Intelligence Regulation stress the importance of transparency. However, the technical complexity of LLMs makes it difficult for users to understand how their data is processed, stored, and used, complicating their ability to exercise rights such as the right to erasure.

As a potential solution to enhance compliance with RTBF in the age of LLMs, several strategies can be considered[14].

a) Data Suppression Technologies: Developing algorithms that allow AI systems to selectively forget specific information could help align LLM operations with RTBF requirements without compromising their functionality.

b) Impact Assessments: Conducting thorough assessments to identify privacy risks associated with LLM deployment can help mitigate potential breaches of the RTBF

c) MultidisciplinaryCollaboration:Engaginglegalexperts,AIdevelopers,andregulators in discussions can foster practical solutions that respect both technological advancements and individual rights.

Challenge of Data Management's Technical Complexity

When organizations want to remove data, they encounter major technical challenges. It can be challenging to find and remove all instances of an individual's data. Because personal information is frequently dispersed throughout numerous systems, both on-premise and cloud- based. Regulatory exemptions might also make it more difficult to decide what information should be kept and what can be removed. Further more, blockchain technology is unchangeable; it directly contradicts RTBF. A blockchain's cryptographic nature prevents data from being changed or removed once it has been recorded there. Although blockchain holds promise for several industries, its immobility makes it difficult to comply with RTBF requests.

[13] The Right to be Forgotten in the Age of Artificial Intelligence, available at: https://letslaw.es/en/right-to-be-forgotten-artificial-

[14] *Supra*

The negative side of the right to be forgotten

“[Public] libraries should be open to all–except the censor.[15]-John F. Kennedy

Everything has its advantages and disadvantages. This right also has its disadvantages. Free speech organizations and supporters warn that the “right to be forgotten” online is in danger of being transformed into a tool of global censorship. It is argued that an RTBF will result in a sanitized version of history where uncomfortable truths will be erased. Removing information from the Internet conflicts with the open nature of the Web and the free flow of information, and it can compel web hosts to rewrite history. An RTBF can have a chilling effect on journalism and media houses not to publish the stories which could lead to demand removal of information, or journalists could face legal repercussions[16]. RTBF tends to limit fearless journalism, inhibiting the flow of information in the public interest. It is all right for the people to not be defined by previous circumstances. The RTBF creates a conflict between individual privacy rights and the public's interest in accessing information. Courts often struggle to find a balance, leading to in consistent rulings that can favour personal privacy at the expense of public knowledge. This inconsistency can create legal uncertainty and undermine trust in judicial systems. Further more, individuals can abuse this right by demanding their negative but information be removed, which can mislead people about the irreality, especially in the political arena where most criminal-background individuals dominate the political game.

Conclusion

The right to be forgotten is in the infant stage in India, and it will take some years to become fully applicable and understandable by the common people of India. With the enactment of the DPDP Act, 2023, along with DPDP Rules, 2025, a new horizon is set to be established regarding the right to be forgotten, with its indirect mention under Section 12. Comprehensive legislative measures tailored to the unique socio-cultural and technological landscape of India are necessary for fully realizing the potential of this right. The legal framework must balance individual privacy rights with the public's right to information, ensuring that the "Right to be Forgotten" does not become a tool for censorship or rewriting history. This requires clear guidelines, rigorous oversight, and a commitment to upholding freedom of expression. India can learn from global experiences, such as the European Union's General Data Protection Regulation (GDPR), and adapt its approach to suit its own domestic needs, including addressing issues of digital illiteracy, data management complexities, and resource constraints. Key to successful implementation will be the establishment of a robust and independent regulatory authority to oversee data processing and enforce compliance. Additionally, the government and stakeholders must prioritize public awareness campaigns to educate citizens on their data rights and the prospective technological challenges.

To summarize, the right to be forgotten represents a critical component of the evolving discourse on privacy in the digital age, but its journey in India has just begun. Through proper policymaking, innovative technology, and public involvement on a large scale, India can fashion a structure that not only safeguards individual privacy but also encourages a fair and open digital system. In an age where data constitutes one of the most prized commodities, protection for it in this manner, keeping foresight as well as responsibility in focus, would define India's respect towards its citizenry's rights as well as core values.

[15] Hunter Criscione, “Forgetting the Right to be Forgotten: The Everlasting Negative Forgetting the Right to be Forgotten: The Everlasting Negative Implications of a Right to be Dereferenced on Global Freedom in the Wake of Google v. CNIL” 32.2 Pace International Law Review 316 (2020).

[16] Right to beForgotten available at:https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-be-forgotten-7(last visited on January 20, 2025).

LEGAL CHALLENGE OF CYBERBULLYING AND ONLINE HARASSMENT: A COMPARATIVE STUDY

Roushan Kumar
LLM Student, South Asian University, New Delhi

ABSTRACT

The rise of digital platforms has brought both positive and negative impacts, with one of the more alarming consequences being the prevalence of cyberbullying and online harassment. These behaviours not only undermine individual well-being but also present complex legal challenges across various jurisdictions. This comparative study aims to analyse the legal responses to cyberbullying and online harassment in different countries, focusing on their definitions, enforcement mechanisms, and legal effectiveness.

Key words: *Cyberbullying, jurisdiction, Online harassment, digital world.*

Introduction

One of the most common and concerning types of cybercrime is Phishing involves cybercriminals using deceptive tactics to trick individuals into revealing personal information, such as passwords, bank details, or social security numbers. This is typically carried out through fraudulent emails, websites, or messages that appear to be from trusted sources, like a bank, a social media platform, or even a colleague. The goal is to convince the victim to click on a link or download an attachment that either installs malware on their device or directs them to a fake website designed to steal their sensitive information. Phishing attacks often look incredibly convincing, with email addresses that appear legitimate and messages that mimic the tone and formatting of official communications. For example, a phishing email might claim to be from your bank, alerting you to unusual activity on your account, and prompting you to “verify” your account by clicking a link. The link might lead to a fake website designed to look like the bank's actual site, where you are asked to enter sensitive information. Another form of phishing is spear phishing which is more targeted. Instead of casting a wide net, spear phishing is tailored to a specific individual or organization. Attackers often research their target to craft more personalized messages, making it harder for the victim to recognize the threat. Phishing is a serious concern because it can lead to financial loss, identity theft, or unauthorized access to sensitive information, such as corporate data. To protect against phishing, individuals should be cautious of unsolicited messages, verify the legitimacy of any requests for personal information, and use multi-factor authentication to add an extra layer of security.

Online Harassment

Online harassment refers to the use of digital platforms, such as social media, websites, emails, and messaging apps, to intentionally harm, intimidate, or distress individuals or groups. It is a broad term that encompasses a variety of abusive behaviors, including cyberbullying, stalking, defamation, and the spreading of harmful content[1]. As the internet becomes increasingly integrated into daily life, online harassment has emerged as a significant issue, affecting millions of people worldwide, particularly vulnerable groups such as women, children, and marginalized communities.’

Types of Online Harassment

1. Cyberbullying: One of the most common forms of online harassment, cyberbullying typically targets children or teenagers. It includes behaviours such as sending threatening messages, spreading false rumours, posting humiliating photos or videos, and deliberately excluding someone from online social groups.

[1] Pavan Duggal, "Cyber Laws: A Guide to Internet Law in India", p.68.

Cyberbullying can lead to severe emotional and psychological consequences for victims, including depression, anxiety, and even suicide.

2. Trolling: This involves deliberately provoking or upsetting others by posting inflammatory, offensive, or controversial content. Trolls often seek to create conflict or engage in malicious debates, targeting individuals or entire groups for the purpose of amusement or to gain attention. While trolling may seem less serious than other forms of harassment, it can still cause significant distress to victims.

3. Stalking: Online stalking occurs when an individual continuously monitors or follows another person's online presence in a way that invades their privacy or causes distress. This can include obsessively tracking someone's social media accounts, repeatedly sending unwanted messages, or even attempting to track the victim's physical location through digital means[2]. Cyberstalking can have a profound psychological effect on the victim, leading to feelings of paranoia and fear.

4. Doxxing: Doxxing involves the public release of private, identifiable information about someone without their consent, such as their address, phone number, or email. The intent is often to cause harm, incite harassment, or expose the victim to dangerous situations. Doxxing can have serious real-world consequences, including threats of physical harm, identity theft, and financial fraud.

5. Revenge Porn: The non-consensual sharing of intimate images or videos, often by a former partner, with the intention of humiliating or degrading the victim, is another form of online harassment. Revenge porn can destroy the victim's reputation and lead to significant emotional trauma.

Impact of Online Harassment

The effects of online harassment can be long-lasting and severe. Victims often experience emotional distress, which may manifest as anxiety, depression, and low self-esteem. In some extreme cases, online harassment has led to suicidal thoughts or actions. Moreover, harassment can extend beyond the digital space, with perpetrators seeking to harm victims in person, for example, through stalking or doxxing. The anonymity provided by the internet often amplifies the aggressiveness of harassers, making it easier for them to escape accountability. Harassers can target victims anonymously or under fake identities, which makes it harder for law enforcement and victims to track them down.

Legal Framework and Response

Many countries, including India, have enacted laws to address online harassment, though the effectiveness of these laws varies. For example, in India, the Information Technology Act, 2000, criminalizes acts such as cyberstalking, identity theft, and the distribution of obscene material. Sections of the Indian Penal Code (IPC)[3], such as those related to defamation, criminal intimidation, and voyeurism, can also be invoked in cases of online harassment. Despite these laws, victims often face challenges when attempting to seek justice. Many are unaware of their legal rights, and the anonymity of online platforms can make it difficult to identify perpetrators. Additionally, online harassment may cross jurisdictions, complicating enforcement.

Combating Online Harassment

To effectively combat online harassment, a multi-faceted approach is required. This includes stronger legal frameworks, better enforcement of existing laws, and a greater focus on digital literacy and awareness. Social media platforms and tech companies also play a crucial role in addressing online harassment by implementing reporting mechanisms, moderating harmful content, and preventing the creation of anonymous accounts that facilitate harassment.

[2] V. S. Natarajan, “Digital Governance: Managing Cybersecurity and Cyber Law”, p 89.

[3] Indian Penal Code 1860.

Education campaigns to raise awareness about the impact of online harassment and encourage respectful online behaviour can also help reduce the occurrence of these harmful activities. Finally, providing better support for victims, such as counselling services and legal aid, is essential in helping them recover from the trauma of online harassment.

Cyberbullying

Cyberbullying in India has become a serious issue in recent years, particularly with the rapid increase in internet usage and social media platforms. With millions of people, especially young individuals, gaining access to smartphones and the internet, the rise of online harassment has grown at an alarming rate. Cyberbullying refers to the use of digital platforms to harass, threaten, or manipulate individuals, often leading to emotional distress, depression, and in extreme cases, even suicide.

One of the most common forms of cyberbullying in India includes spreading false rumours, posting offensive or abusive comments on social media, sending threatening messages, and sharing private images or videos without consent. School children and teenagers are the primary victims, but adults, especially women, are also frequent targets of cyberbullying. This can be through social media platforms like Facebook, Instagram, Twitter, or even messaging apps such as WhatsApp.

The impact of cyberbullying on victims in India can be devastating. The psychological toll can include anxiety, depression, low self-esteem, and social withdrawal. Victims often feel helpless due to the anonymity that the internet provides to the perpetrators. Furthermore, there is a lack of awareness regarding the legal remedies available to victims, and law enforcement often struggles to keep up with the complexities of cybercrimes.

The Indian government has recognized the issue and introduced various laws to combat cyberbullying, such as the Information Technology Act, which includes provisions against cyber harassment. However, enforcement remains a challenge, and many victims are unaware of their rights and the support available to them.

To tackle this problem, there is a need for greater public awareness, stronger laws, better online etiquette, and a proactive role from social media companies in monitoring and preventing cyberbullying.

Law related to cyberbullying

In India, cyberbullying is addressed under several legal provisions aimed at curbing online harassment, threats, and the misuse of digital platforms. While specific laws targeting cyberbullying are limited, various sections of the Indian Penal Code (IPC), the Information Technology Act (IT Act), and other statutes are employed to protect victims and punish perpetrators.

The Information Technology Act (IT Act)

The IT Act, which deals with cybercrimes, is one of the primary pieces of legislation to combat cyberbullying. While the Act doesn't specifically mention cyberbullying, several sections under it address cyber harassment and related crimes:

Section 66A (before it was struck down): Previously, Section 66A of the IT Act penalized sending offensive messages via communication service, etc. It was often invoked in cases of online harassment and cyberbullying. However, the Supreme Court struck it down in 2015, declaring it unconstitutional, as it violated the right to freedom of speech.

Section 66C (Identity theft and impersonation): This section penalizes the use of someone's identity without consent, which is a common tactic in cyberbullying, where perpetrators often impersonate others to defame them online.

Section 66E (Violation of privacy): This provision addresses the unlawful capturing, publishing, or transmitting of an individual's private information or images. In cases of revenge porn or sharing private photos without consent, this section provides a legal remedy for the victims of cyberbullying.

Section 67 (Obscene content): This section criminalizes the transmission or publication of obscene material in electronic form. Cyberbullying often involves the distribution of inappropriate or abusive content aimed at defaming a person. Offenders may face imprisonment and fines under this section.

Section 72 (Breach of confidentiality and privacy): This provision makes it an offense for a person to disclose personal information obtained through electronic communication, which is central to many cyberbullying cases where personal data is misused.

The Indian Penal Code IPC ,1860

The IPC also provides a framework for addressing cyberbullying related offenses. Several sections of the IPC can be invoked depending on the nature of the bullying:

Section 499 (Defamation): If a person's reputation is damaged through false and defamatory statements on social media or other platforms, they can file a complaint under this section. Cyberbullying often includes character assassination or spreading rumors, which may fall under defamation.

Section 506 (Criminal intimidation): This section addresses threats made to cause harm or fear. Cyberbullying often involves threats of physical harm or emotional distress, making this section relevant for cases involving threats of violence or harm.

Section 507 (Criminal intimidation by anonymous communication): Cyberbullying often occurs through anonymous accounts or accounts that do not identify the perpetrator. This section specifically criminalizes threats made anonymously, which is common in cyberbullying incidents.

Section 66 of the Information Technology Act, 2000, essentially deals with "computer related offences", meaning if someone dishonestly or fraudulently performs any act mentioned in Section 43 of the IT Act, they can be punished with imprisonment up to three years, a fine of up to five lakh rupees, or both; essentially criminalizing acts like hacking with malicious intent; the terms "dishonestly" and "fraudulently" are defined according to the Indian Penal Code IPC ,1860

Section 354C (Voyeurism): This section penalizes the act of voyeurism, including the non-consensual capturing of intimate images or videos. Cyberbullying frequently involves such acts, and this section provides legal recourse for victims of image-based abuse.

Section 509 (Word, gesture, or act intended to insult the modesty of a woman): In cases of cyberbullying targeting women, particularly those involving verbal abuse or insults, Section 509 can be invoked to punish offenders who insult a woman's modesty through online channels.

The Protection of Children from Sexual Offences (POCSO) Act, 20128

Cyberbullying cases involving minors are also subject to the provisions of the POCSO Act, especially when the bullying involves sexual harassment, exploitation, or abuse online. Cyberbullying often includes sending inappropriate messages or exploiting children through online platforms. The POCSO Act aims to protect children from any form of sexual harassment, and the involvement of technology has made it increasingly relevant in cases of online abuse.

The Role of the Police and Cyber Cells

India's law enforcement agencies, including cybercrime cells, play a crucial role in tackling cyberbullying. Most major cities have dedicated cybercrime units or cyber cells that investigate cases of online harassment. However, victims often face challenges when reporting cyberbullying due to a lack of awareness, slow law enforcement processes, and insufficient technical expertise in dealing with sophisticated online crimes.

Challenges and Need for Reforms

Despite the presence of these legal provisions, several challenges remain in tackling cyberbullying effectively. These include the anonymity offered by the internet, the jurisdictional complexities of cybercrimes (especially when perpetrators are outside India), and the slow pace of legal proceedings. There is also a lack of specific laws that directly address cyberbullying, leaving victims to rely on general provisions that might not fully address the nuances of online harassment. Further reforms and stricter enforcement are needed to protect individuals from cyberbullying. Public awareness campaigns about legal rights, increased accountability for online platforms, and enhanced training for law enforcement could help improve the response to this issue.

Difference between online harassment and cyberbullying

Online harassment and cyberbullying are both forms of digital abuse, but they differ in terms of their scope, intent, and impact. While both involve the use of digital platforms to cause harm, they manifest in different ways and may affect individuals differently. Understanding the distinctions between these two terms is crucial in identifying and addressing each type of behaviour.

i) Online Harassment: This is a broad term that refers to any abusive behaviour carried out over digital platforms, such as social media, emails, messaging apps, or websites. Online harassment includes a wide range of harmful actions, such as cyberstalking, doxxing, trolling, and sending threatening or obscene messages. It can target individuals or groups, and the perpetrator may not necessarily have a personal relationship with the victim. Online harassment can be one-time incidents or ongoing abuse, and it may occur across multiple digital platforms.

Example: A person might receive repeated threatening emails from an unknown individual who has accessed their personal information. This behaviour is online harassment, as it involves an attempt to intimidate or harm the victim, without any prior relationship between the victim and the harasser.

ii) Cyberbullying: Cyberbullying is a specific form of online harassment primarily targeted at children and teenagers. It often involves repeated behaviour intended to intimidate, hurt, or embarrass the victim. Cyberbullying typically takes place on social media platforms, chat rooms, or through text messages. It often involves direct communication or public humiliation, with the intent to diminish the victim's self-esteem or social standing. The victim and perpetrator often have a personal relationship, such as being classmates or friends, and the bullying tends to be more persistent.

Example: A teenager might receive constant negative comments, memes, or even threats on their Instagram account from classmates, aimed at mocking their appearance or spreading rumors about them. This ongoing harassment, intended to emotionally harm the victim, is an example of cyberbullying.

iii) Intent and Motivation

The intent behind online harassment can vary. Perpetrators may be motivated by a desire for power, revenge, or simply to cause emotional distress. Harassment may also be driven by ideological, political, or financial motives. The harasser may not have a personal relationship with the victim and may engage in the behaviour out of malice or a desire to incite fear or discomfort.

Example: A journalist could be subjected to online harassment by anonymous individuals who disagree with their political views. These individuals may send the journalist hateful messages, threats, or even hack into their social media accounts to intimidate them and silence their opinions. The motivation is rooted in opposition to the journalist's views, rather than a personal vendetta.

Cyberbullying: The intent behind cyberbullying is typically to humiliate, isolate, or emotionally harm the victim. Often driven by peer pressure, jealousy, or a desire to maintain social status, the perpetrator might target the victim repeatedly because of their perceived differences, such as their appearance, behaviour, or social standing. The bullying can be fuelled by personal animosity, and the victim may be targeted due to their vulnerability or because they are seen as an easy target for ridicule.

Example: In a high school setting, a student might spread false rumours about a peer to make them a laughingstock among classmates. The bullying is fuelled by a desire to elevate the bully's own social status at the expense of the victim's emotional well-being.

iv). Duration and Frequency

Online Harassment: The frequency and duration of online harassment can vary widely. It may be a one-time incident or an ongoing situation. Harassment does not always have to be repetitive, but it often escalates over time, especially if the harasser feels they can act with impunity.

Example: A woman might be stalked online by an ex-partner who repeatedly monitors her social media accounts, posts invasive comments about her private life, and sends threatening messages. This harassment may happen intermittently but can last for months or even years, depending on the situation.

v) Legal and Social Implications[4]

Both online harassment and cyberbullying can have serious consequences for the victim, including emotional distress, depression, and, in extreme cases, suicidal thoughts. Legally, both behaviors are often treated similarly, and many countries have laws in place to protect victims of both online harassment and cyberbullying. However, cyberbullying, especially when it involves minors, often leads to stricter school policies and legal repercussions for the bully's parents or guardians. Online harassment, on the other hand, may result in criminal charges, including stalking, defamation, or identity theft.

United States

In the United States, cyberbullying and online harassment are addressed through a combination of federal and state laws. While the U.S. lacks a specific federal law exclusively governing cyberbullying, several states have enacted their own statutes. For example, California's anti-bullying law provides a legal framework for addressing harassment that occurs through electronic means. At the federal level, the Communications Decency Act (CDA) 11 Section 230 provides immunity to internet service providers, limiting their liability for user-generated content. This has been a point of contention as it makes it challenging to hold platforms accountable for the spread of harmful content. In response to the increasing incidents of cyberbullying, Congress has proposed the "STOP Cyberbullying Act," which aims to establish a national legal standard. However, the key legal challenge in the U.S. remains balancing freedom of speech with protection from harm, as there is often ambiguity regarding what constitutes protected speech versus harmful behavior.

United Kingdom

In the UK, the legal approach to cyberbullying and online harassment is more structured. The Malicious Communications Act 1988 and the Communications Act 2003 are commonly used to prosecute online harassment, criminalizing the sending of threatening or offensive messages. Additionally, the Protection from Harassment Act 1997 has been adapted to cover online harassment, making it an offense to cause distress or alarm through electronic means. The UK also introduced the "Online Safety Bill" in 2021, aimed at regulating

[4] https://www.unicef.org/end-violence/how-to-stop-cyberbullying

harmful content on social media platforms, placing greater responsibility on tech companies to take down abusive material and protect users. However, the UK faces challenges in keeping up with the rapid evolution of technology, as new platforms continuously emerge, and defining what constitutes harmful content can be subjective.

Australia

Australia has developed comprehensive laws to combat cyberbullying, with the Cyberbullying and Cybercrime Bill 2016 making online bullying a criminal offense under certain conditions. The country has also set up a national online complaints' mechanism via the eSafety Commissioner, who can issue removal notices for harmful content and even take legal action against the offenders in extreme cases. One of the unique features of Australian law is its focus on the prevention of harm by encouraging platforms to respond promptly to complaints and empowering individuals to report online harassment. Despite these robust measures, a significant challenge is the global nature of the internet, which often makes enforcement difficult across national borders.

INDIA

In India, cyberbullying and online harassment are addressed through provisions in the Information Technology Act, 2000 (IT Act), which criminalizes cyberstalking, identity theft, and cyber harassment. The Indian Penal Code (IPC) also has relevant sections, such as Section 66A (which was struck down by the Supreme Court in 2015) and Section 354D (dealing with stalking). While India has made progress in criminalizing online harassment, the legal framework faces challenges in terms of awareness, enforcement, and the speed at which cases are processed. Additionally, the lack of a comprehensive, uniform law specifically targeting cyberbullying remains a gap.

Here are a few more notable cases involving cyberbullying and online harassment that have caught public attention:

In the case of *Hannah Smith* (2013), Hannah Smith, a 14-year-old from Leicestershire, England, was subjected to intense cyberbullying through social media platforms, particularly Ask.fm. After months of abusive messages, including threats and cruel comments, Hannah tragically took her own life. Hannah's death led to increased scrutiny of Ask.fm, with many accusing the site of failing to act on complaints of bullying. Her case contributed to the platform being banned in some countries, and it spurred further discussions about the responsibility of social media companies in addressing bullying..

In the case of *Monica Lewinsky* (1998-1999) Monica Lewinsky, a former White House intern, became the target of widespread public shaming after her affair with President Bill Clinton became publicly known. Although this case predates the modern concept of "cyberbullying," it was a significant example of online harassment. The affair was ridiculed in countless memes, websites, and forums, resulting in immense public humiliation. Lewinsky became the subject of relentless online mockery, which had lasting emotional and psychological effects. Over time, she used her experience to advocate for anti-bullying efforts, especially regarding the harmful effects of public shaming and cyber harassment. Her advocacy work continues to highlight how online harassment can shape a person's life.

In the case of *Caroline Criado-Perez* (2013), Caroline Criado-Perez, a British feminist and campaigner, faced severe online harassment after successfully campaigning for a woman (Jane Austen) to appear on the Bank of England's £10 note. She was flooded with threatening messages on Twitter, including violent threats and rape threats. The harassment was so severe that Criado-Perez contacted the police, and two men were later arrested and charged. This case led to changes in UK law regarding online harassment and prompted calls for social media companies to take greater responsibility for monitoring and acting against abusive content.

In the case of *Justine Sacco* (2013), Justine Sacco, a former PR executive, made an insensitive tweet before boarding a flight to South Africa, which quickly went viral. The tweet was widely condemned as racist, and she was subjected to a wave of online harassment, including death threats. Sacco's life was significantly impacted by the viral backlash, which continued even after she was fired from her job. The incident sparked debates about cancel culture, online mob mentality, and the dangers of social media's viral nature. It also highlighted the consequences of making poorly thought-out comments online and the quickness with which people can be vilified.

In the case of *Zoe Quinn* (2014), Zoe Quinn, a video game developer, became the target of a hate campaign after her ex-boyfriend published a series of blog posts accusing her of unethical behavior within the gaming industry. The incident sparked the "Gamergate" movement, which involved extensive harassment, including threats of violence, doxxing, and sexist comments directed at Quinn and other women in the gaming community. The harassment Quinn faced had a significant personal toll, including threats to her life and safety. The case led to increased attention on the role of social media in facilitating harassment, especially in online communities. It also highlighted the broader issue of misogyny in gaming culture. Quinn became an advocate for addressing harassment in online spaces.

Cyberbullying and online harassment continue to be significant issues in India, affecting individuals of all ages, particularly teenagers, young adults, and women. Here are some recent cases related to cyberbullying and online harassment in India:

In the case of *Disha Ravi* (2021); Disha Ravi, a climate activist, was arrested in 2021 for her involvement in creating and sharing a "toolkit" related to the farmers' protest in India. While her arrest was politically charged, it quickly became evident that she faced significant online harassment. Social media was flooded with hateful comments, threats, and sexist remarks aimed at her. She was targeted for speaking out on issues of social justice, particularly by those who disagreed with her political stance. The case attracted widespread attention to the issue of online harassment, particularly targeting women activists and young voices. Despite her legal challenges, the case brought attention to the growing issue of online violence, with many social media users rallying in her defense. The incident also highlighted the need for stronger laws and protection for women and activists online.

In case of *"Bulli Bai"App* (2021); a notorious app called *Bulli Bai* appeared on GitHub, where a group of individuals created an online auction platform for Muslim women, posting their photos without consent and describing them in offensive terms. The women featured on the app were primarily prominent social media personalities, journalists, and activists. The app was designed to harass and objectify them, with the clear intention of humiliating Muslim women. The *Bulli Bai* app sparked outrage and was widely condemned for promoting online harassment, misogyny, and communal hate. Several individuals were arrested for their involvement in creating and promoting the app, including a student from Bengaluru. The incident led to discussions around the lack of accountability of tech platforms, the need for stricter cybersecurity laws, and the vulnerability of women to online harassment in India.

In case of *Shreya* (2021); Shreya, a student from Delhi, became the target of online harassment after her intimate photos were shared without her consent. The photos were leaked on social media, and Shreya was relentlessly bullied and humiliated online by a large number of people, many of whom were classmates or acquaintances. Shreya's case highlighted the issue of "revenge porn" and non-consensual image sharing, a growing problem in India. It also exposed the vulnerabilities of young women to online exploitation. Shreya's case received media attention, and there were calls for stricter legal measures to combat such forms of cyberbullying, including calls to strengthen the Information Technology Act and other laws related to privacy and digital harassment.

In case of the *"Sulli Deals"*(2021), a website called Sulli Deals was launched on GitHub, where photographs of Muslim women were uploaded without their consent, and they were listed for "auction." The app targeted Muslim women, presenting them as objects to be humiliated and dehumanized. Many of the women featured were active on social media or were well-known public figures. The incident led to widespread public outrage and protests, especially among the Muslim community in India. The police took action , leading to arrests in the case. The "Sulli Deals" incident again brought attention to the harassment and objectification of women online, especially those from marginalized communities. It also led to greater scrutiny of online platforms and the role of tech companies in preventing such abuse.

In case of *Ayesha* (2020), Ayesha, a student from Uttar Pradesh, was targeted by online bullies after a photo of her was shared on social media without her permission. The photo went viral, and Ayesha received numerous offensive comments and threats online, including threats of sexual violence. The harassment continued for weeks, deeply affecting her mental health. This case emphasized the dangers of online privacy violations, particularly for women and girls, and the serious impact of cyberbullying. Ayesha's family approached the police, who took swift action to identify the perpetrators. It was a reminder of the need for better awareness and education around online privacy, and it sparked discussions on how to protect individuals from such incidents.

Legal Developments

Recent cases of cyberbullying and online harassment in India have triggered significant discussions about the legal framework surrounding these issues. Some key legal measures include:

1. *The Information Technology Act, 2000*: This Act deals with offenses related to online harassment, including cyberbullying and data privacy violations. Sections 66A (which criminalized sending offensive messages) and 66E (related to violation of privacy) have been invoked in several cases, though Section 66A was struck down by the Supreme Court in 2015 due to its vague wording.

2. *Cyber Crime Cells and Online Reporting*: Various state police departments in India have set up cybercrime cells to tackle online harassment and cyberbullying. There are also initiatives like the National Cyber Crime Reporting Portal, launched by the Ministry of Home Affairs, which allows people to report cybercrimes, including online harassment.

3. *Increased Advocacy for Women's Safety Online*: Activists and organizations are pushing for more stringent laws to protect women from cyberbullying and harassment. These include proposals to improve the speed of legal responses to cybercrimes and to hold social media platforms accountable for hosting abusive content. These cases serve as a reminder of the urgent need for effective legal protections, increased awareness, and better moderation on digital platforms to protect individuals from the devastating effects of cyberbullying and online harassment. These cases show how pervasive and damaging cyberbullying and online harassment can be, affecting individuals across different spheres of life—whether they are teenagers, professionals, or public figures. They also underscore the urgent need for stronger protections and better management of online spaces.

Conclusion

The legal response to cyberbullying and online harassment varies significantly across jurisdictions, shaped by cultural, technological, and political factors. While some countries like the UK and Australia have developed specific, proactive legal frameworks, others such as the U.S. rely on a patchwork of state laws and a reluctance to limit platform immunity. Global cooperation is essential in addressing the cross-border nature of cyberbullying, especially when offenders often operate anonymously. Ultimately, while legal frameworks are evolving, more comprehensive, adaptable, and universally applicable laws will be necessary to combat. Online harassment is a serious and growing issue in today's digital world. It has the potential to cause significant psychological harm, disrupt lives, and, in extreme cases, lead to physical harm. While legal frameworks and social media companies have made efforts to combat online harassment, more needs to be done to protect individuals from digital abuse. Raising awareness, improving laws, and providing support for victims are crucial steps in addressing this issue and creating a safer online environment for everyone. While India has a legal framework in place to address cyberbullying, its effectiveness depends on awareness, timely enforcement, and overcoming the challenges posed by the rapidly evolving digital landscape. Strengthening the laws and increasing their application is essential to ensure that victims of cyberbullying receive justice and protection. While online harassment and cyberbullying overlap in many ways, they are distinct concepts. Online harassment is a broad category that includes various forms of digital abuse, which can be directed at individuals of all ages and for various reasons. Cyberbullying, on the other hand, is a specific type of harassment that primarily targets children and teenagers and is usually more repetitive and focused on emotional harm. Both require serious attention and intervention, as their impacts on victims can be devastating. The growing prevalence of digital platforms underscores the need for stronger regulations, education, and support systems to combat both online harassment and cyberbullying effectively.

REFERENCE

1. "Cyber Law in India" by Dr. Suresh T. Vishwanathan.
2. "Cyber Laws: A Guide to Internet Law in India" by Pavan Duggal
3. "Introduction to Cyber Law" by N. P. Singh
4. "Cyber Law in India" by Farooq Ahmad
5. "Law Relating to Cyber Crime & Information Technology" by Dr. Sandeep K. Shukla
6. "The Law of Cyber Crimes and Internet Security" by Farooq Ahmad.
7. "Cyber Law and E-Commerce" by S. R. Sharma.
8. "The Indian Cyber Law" by Dr. P. K. Agarwal
9. "Cyber Law and Ethics" by Arvind Narain.
10. "Digital Governance: Managing Cybersecurity and Cyber Law" by V. S. Natarajan

Legislations

i) IPC, 1860
ii) IT ACT ,2000
iii) Protection from Harassment Act, 1977.

Journal

https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications decency-act-1996
https://www.unicef.org/end-violence/how-to-stop-cyberbullying
https://www.stopbullying.gov/cyberbullying/what-is-it
https://reportandsupport.durham.ac.uk/support/what-is-online-harassment

CORPORATE TAX REFORMS IN THE DIGITAL ECONOMY: INTERNATIONAL COORDINATION AND CHALLENGES

Adarsh Tripathi
Student, Manikchand Pahade Law College, Aurangabad

ABSTRACT

This research paper explores the various issues associated with corporate tax reforms, in consideration of the digitized structure of the economy. The paper examines the modern structure of global taxation systems and the OECD's BEPS project, including Pillar One, which introduces new rules for nexus and profit allocation, and Pillar Two, which implements a global minimum tax. It addresses various approaches, such as India's Equalization Levy and the EU's proposed Digital Services Tax (DST), highlighting that international relations could position digital taxation as a new source of trade tensions and market divides.

A precedent, such as *Google India Pvt Ltd v. Commissioner of Income Tax*, underscores the high number of national taxation measures that conflict with global standards, exacerbating cross-jurisdictional complications. The secondary analysis explores the methodological, economic, and political perspectives of international tax reforms, focusing on self-interested policies, administrative concerns, and market distortions.

The paper recommends that policy authorities collaborate to create a unified system that aligns with the evolving needs of the digital economy while preventing tax evasion and promoting international tax harmonization.

Key words: *Digital Economy, Corporate Tax Reform, International Coordination, OECD, Digital Taxation.*

Introduction

Changes in the digital economy have shifted the strategic organizational character of different enterprises by applying dynamism kin to long-established businesses seen more as an evolution rather than revolution which is worldwide, systematic and innovative. Today's digital enterprises let some of the leading technologic corporations operate and generate tax revenues in various countries with no tangible location. This situation often results in a low or non-existent 'nexus' and 'permanent establishment' as required by traditional tax laws[1]. The advancement of this concept represents, however, a set of problems for national tax systems, which are, to a great extent, based on 20th century concepts that primarily focus on the direct taxation of profits in accordance with physical presence. The increased disparity between contemporary digital business models and conventional tax systems has created conditions in which some MNCs have been able to avoid taxes and minimize their rates of payment through BEPS. These practices not only decrease national tax collections but also raise new urgent issues concerning justice and equity in international taxation. Therefore, policymakers across the globe have found the need to undertake comprehensive corporate tax reforms.

At the very heart of this talk, there is the issue of international cooperation, since this approach, which is based on nation-state level measures, has been found to be inefficient and, in some cases, damaging. Thus, the Organisation for Economic Co-operation and Development (OECD) started a programme of work to address a range of issues pertaining to the international tax system under the BEPS project with focus on taxation of the digital economy[2]. The OECD has estimated that as much as 4-10% of total worldwide corporate income tax revenue, or between $100 billion to $240 billion annually, is at risk from BEPS[3]. This is so especially because

[1] Ana Luísa Gonçalves Novais, Ana Oliveira Anabela Susana de Sousa Gonçalves, Elif Nazli Birgi, Francisco Andrade de Portugal Isabel Fidalgo da Silva, João Novo Faria Lages, João Sérgio Ribeiro José Pedro Correia Fernandes, Maria João Maurício, Tilmar W. Goos, Yi Zheng, 'Selected Essays on International Business Law' (University of Minho, October 2018) <7. Selected Essays on International Business Law.pdf> accessed 10 November 2024

[2] Monica Gianni, 'OECD BEPS (In)Action 1: Factor Presence as a Solution to Tax Issues of the Digital Economy' (2018) 111 JSTOR < ssrn-3211971.pdf> accessed 10 November 2024

[3] Haiyan Xu, 'The Reflection on the Magnitude and Disasters of BEPS Schemes' (2019) 10(4) Beijing Law Review < The Reflection on the Magnitude and Disasters of BEPS Schemes> accessed 10 November 2024

developing countries are more greatly negatively affected due to the fact that they source for most of their income from corporate taxes. To tackle this OECD's sweeping two- plan approach, Pillar One and Pillar Two, aims to reform the current taxonomy of MNC profit allocation, reallocate taxing rights across countries, and implement global minimum taxation to prevent base erosion and profit shifting. As of 2024, over 140 countries have agreed, in principle, to implement the OECD's two-pillar solution[4].

Pillar One shifts the taxing rights to market jurisdictions and is for MNCs with a global turnover of more than €20 billion and profit above 10%[5]. This shift is supposed to help contain problems with the nexus standard, where some digital firms have generated large revenues from markets that demand high taxes, while paying little or no taxes. However, there is still a problem in measuring this share of these profits and more so where their countries counter economics' interests.

Within Pillar Two, there is an explicit minimum rate intending to eliminate base stripping of 15% for MNCs with consolidated revenue over €750 million[6]. However, Average global corporate tax rate is about 23.45% in 2023 and low corporate tax rates are offered in countries like Ireland 12.5 % thus attracting more MNC's due to a favourable environment[7]. Businesses and Individuals that indulge in tax avoidance strategies employ nations with either a zero level or very low overall taxation rate like the Cayman Islands and Bermuda since countries with low taxation rates are very suitable for techniques like profit shifting or improving profits through cross border activities.

This is facilitated by the creation of a minimum tax standard. This measure directly addresses the problem of “BEPS” by pressuring countries to compete for FDI through lower corporate tax rates, which in turn enhances existing technology and enables digital and other multinational corporations to engage in more effective tax avoidance. The expected increase in global tax revenues is estimated at $150 billion annually once Pillar Two is fully implemented[8].

Despite this, the following examples show that these kinds of reforms are not easy to implement globally, as some notable court cases in jurisdictions where tax authorities have audited the tax structures of some of the big MNCs demonstrate. For example, Apple in Ireland and Amazon in Luxembourg can be considered typical examples of companies for which the topical question of fair taxation under current legislation is classified by the European Commission as unlawful. In European Commission v. Ireland and Apple Sales International (2020), the Commission sought to make Apple shoulder €13 billion in unpaid taxes, arguing that the tax structure Apple received in Ireland was unlawful state aid because it allowed Apple to avoid paying a near-zero tax rate on all its European profits[9]. However, in 2014, the General Court of the European Union set aside this decision on the legal and technical aspects regarding the interpretation of 'fair' taxation in a system that eludes the various tests aimed at countering the problem of profit shifting.

These cases demonstrate the generally weak state of current tax frameworks and the need to create a unified and coherent standard that will enable different jurisdictions to operate in a unified manner. It is noted that, due to increased variation in the national tax regimes of the intended adopters, there has been a tendency towards what is referred to as “double non-taxation,” whereby digital MNCs are able to avoid taxation in both the home country

[4] 'PwC's Pillar Two Country Tracker provides the status of Pillar Two implementation in different countries and regions' (pwc, 31 October 2024) < OECD Pillar Two country tracker | PwC> accessed 10 November 2024

[5] Roberto Fei, Massimo Moltoni and Gabriele Romeo, 'New Challenges, New Rules: The Global Minimum Corporate Tax' Orizzonti Politici (Bocconi, December 2021) < Microsoft Word - Bozza1_Corporate Tax_integrale 9.docx> accessed 10 November 2024

[6] Reuven Avi-Yonah & Young Ran (Christine) Kim, 'Tax Harmony: The Promise and Pitfalls of the Global Minimum Tax' (2022) 43(3) SSRN < ssrn-4102332.pdf> accessed 10 November 2024

[7] Cristina Enache, ‘Corporate Tax Rates around the World, 2023’ (Tax Foundation, 12 December 2024) < Corporate Tax Rates around the World, 2023> accessed 10 November 2024

[8] Reuven Avi-Yonah, ‘A New Framework for Digital Taxation’ (2022) 63(2) SSRN < ssrn-4068928.pdf> accessed 10 November 2024

[9] Keith O’ Donnell, Samantha Schmitz, Marie Bentley, ‘Apple Case: EU Judges Confirm That The European Commission Had It Wrong’ (Mondaq, 23 July 2020) < Apple Case: EU Judges Confirm That The European Commission Had It Wrong - Tax Authorities - Tax - European Union> accessed 10 November 2024

and the host country[10]. The OECD's proposed reforms aim to address such loopholes, but the effectiveness of these reforms rests on a high level of compliance among different nations, as noncompliance will lead to the weakening of the international taxation system.

The negotiation of these reforms is not easy to accomplish. Those countries that have maintained low corporate tax rates to attract foreign investment through tax-friendly environments may not easily agree to any change in the tax structure that would undermine their competitiveness. Additionally, there has been an increase in the sovereignty argument, as some nations believe that joining the global tax standards may hamper their independence in local taxation policies[11]. Many developing nations primarily rely on tax receipts from traditional multinational corporations (MNCs) with a physical presence, and therefore face unique issues that challenge the current simplistic electronic tax rules, which are primarily geared towards large digital corporations. Moreover, reliance on such instruments can present legal and procedural problems, and such reforms need to be integrated into domestic tax laws to avoid delays and controversies that could hinder the broad-scale implementation of these reforms.

Nonetheless, the efforts being made by international bodies such as the OECD are indicative of the fact that there is increased awareness that conventional tax systems require modifications that can best be sourced through the realities of the digital domain. Given these conceptual and political challenges, this paper presents the objective of critically evaluating the main aspects of the OECD's two-pillar strategy for its feasibility, its likely effects on national tax revenue, and its consequences for economic equality. As part of the discussion, recent cases and national actions in the absence of a generally accepted international policy will be presented, such as the 2% DST on digital companies earning more than £500 million globally, with at least £25 million from UK-based activities and generating £300 million in the first year 2021[12].

The “GAFA” tax (Google, Apple, Facebook, Amazon) at **3%** on revenues from digital services in France which generate revenue approximately €518 million in the year 2022 according to government forecast[13]. Thus, outlining the prospects for practical, legal, and political solutions to international tax issues in this paper will help expand knowledge of the necessity for a concerted response to the taxation challenges of the digital economy.

1. Inadequacy of Traditional Tax Rules for the Digital Economy

The current system of international taxation has been designed to address the traditional ways of operation based on establishing a physical presence in a country to generate income. The traditional concept of PE is foundational, but it becomes almost irrelevant in the digital economy because businesses can engage customers and beneficiaries in a country and make profits without a physical presence. This has created loopholes through which digital corporations can reduce their tax remittances, resulting in revenue losses for countries with large user bases.

According to a 2020 report by the Tax Justice Network, global tax losses due to profit shifting were estimated to be around $245 billion annually[14]. One direct and recent example is Google Ireland Ltd. from the United Kingdom. In its European operations, Google was strategically established to take advantage of Ireland's favourable tax policies and transfer profits to Ireland to escape high-tax countries with high levels of user engagement. The case also shows how digital multinationals can use physical presence conditions to avoid

[10] Zafar Harnekar, ‘The source of income from the sale of goods electronically: an analysis of the division of the taxing rights in cross-border situations’ (University Cape Town, 2016) <The income nexus of the digital economy in a South African context: a case study approach> accessed 10 November 2024

[11] Insop Pak, ‘International Finance and State Sovereignty: Global Governance in the International Tax Regime’ (2004) 10(1) SSRN < International Finance and State Sovereignty: Global Governance in the International Tax Regime> accessed 10 November 2024

[12] Ministry Revenue and Custom, Introduction of the new Digital Services Tax (2019) < Introduction of the new Digital Services Tax - GOV.UK> accessed 10 November 2024

[13] N Marques, PS Onge, G Campan, ‘Taxing the Tech Giants Why Canada Should Not Follow the French Example’ MEI < Taxing the Tech Giants – Why Canada Should Not Follow the French Example> accessed 10 November 2024

[14] ‘The State of Tax Justice 2020: Tax Justice in the time of COVID-19’ (Tax Justice Network, November 2020) < The_State_of_Tax_Justice_2020_ENGLISH.pdf> accessed 10 November 2024

significant taxation. This is why reform should focus on changing the economic presence rule rather than physical presence rule. If tax laws move to the "place of physical presence," then companies would have to pay taxes in the countries where they maintain offices, employees, existence, and other concrete business in one way or another irrespective of their revenue's origin. In this way, firms cannot simply relocate their offices to territories with low tax rates and avoid paying more tax to the countries where operating business is real.

For instance, if Google established a small office in a country with low taxation policies but earned most of its profits from the UK, under the 'physical presence' rule, Google would be taxed in the UK because the company has physical operations there. This ensures that companies contribute fairly to the countries where most of their business activities take place, by reducing tax evasion by the companies.

In response, many jurisdictions are requesting the creation of a taxonomy based on significant economic presence, which would allow them to exercise taxing rights over companies with extensive digital operations in their jurisdictions[15]. This change is intended to update tax legislation by emphasizing the generation of added value instead of depreciated property, notably with reference to digital companies that continuously reconfigure the added values and the places where these values are created. Nonetheless, designing and implementing such a framework still proves complex due to differing views on the meaning of economic presence and possible conflicts with existing ITAs.

2. OECD's Base Erosion and Profit Shifting (BEPS) Initiatives

In 2013, recognizing that current tax regimes presented failures, the OECD headed a new Base Erosion and Profit Shifting (BEPS) project. BEPS seems to be most important in the context of the digital economy because it targets the strategies that enable companies, through international tax planning, to move profits to territories with low taxation. The first pillar of the OECD's plan is the redistribution of taxing rights, known as Pillar One; the second pillar of the OECD's plan is the designed implementation of a global minimum tax, known as Pillar Two[16].

The BEPS initiatives themselves are inventive, although they face major challenges. For example, Pillar One presents the suggestion that multinationals should be taxed in the jurisdiction of their place of residence but also where they have minimal digital presence. However, this new approach lacks a degree of supranational collaboration, which is not easily achieved because of the varying economic and political stakes of sovereign players. Moreover, certain countries, notably Ireland and some countries in the Caribbean region, consider the reforms a threat to their sovereignty and the dismantling of the potential that has attracted multinational investment. Ireland's resistance is rooted in economic self-interest; corporate tax contributes substantially to its GDP, with 2022 figures showing that corporate tax revenues accounted for approximately 27.5% of its total tax intake[17].

The OECD's proposed measures also trip the existing bilateral tax treaties. One of the recent decisions of international tax relocation arises out of the Ireland case: Dell Products Ltd. v. Revenue Commissioners. In this case, Ireland enjoys a good tax policy that channels corporate revenue to the country, which was put under the microscope by the EU on anti-tax avoidance policy. The same can be said about the cases presented, which state that the OECD struggles to make progress due to the opposition presented by the jurisdictions that benefit from the currently existing loopholes[18]. While Pillar Two has the ambitious goal of establishing the minimum tax in order to counter tax base erosion, its enforcement presupposes coordinated legislative amendments that, in spite of the BEPS call, have not seen much action due to the lack of enthusiasm and political resistance.

[15] Colin Clavey, Jonathan Leigh Pemberton, Jan Loeprick, Marijn Verhoeven, 'International Tax Reform, Digitalization and Developing Economics' 16 World Global Group < World Bank Document> accessed 10 November 2024

[16] Reuven Avi-Yonah, Young Ran (Christine) Kim, 'Tax Harmony: The Promise and Pitfalls of the Global Minimum Tax' 43(3) SSRN < ssrn-4102332 (1).pdf> accessed 10 November 2024

[17] Larry McCarthy, 'Corporation Tax – 2022 Payments and 2021 Returns' (CT, May 2023) < Corporation Tax - 2022 payments and 2021 returns> accessed 10 November 2024

[18] Pieter Baert, 'Ireland's tax reforms and the fight against aggressive tax schemes' (European Parliament, June 2022) < Ireland's tax reforms and the fight against aggressive tax schemes> accessed 10 November 2024

3. Challenges in Achieving International Coordination

The consensus on digital tax reforms is a difficult process because the interests of each country are divergent. Some of the developed countries have complained that digital multinationals are not paying taxes commensurate with the revenues they generate and thus have called for higher taxes on corporations; the low-tax countries have opposed any changes that might eat into their models. For instance, according to a 2022 report by the OECD, large tech companies have seen profit margins between 15% to 30%, while effective tax rates often fall below 10%, far beneath the corporate average of 23.5% in many developed economies[19]. Additionally, the emerging nations have an objection that the planned methods of distribution are not very favourable for them: these countries often act as large consumers of digital services approximately 60% of the global digital consumer base, obtaining major revenues for digital businesses[20].

Digital Service Tax (DSTs) are other acts of recourse that have only served to exacerbate regulatory coordination issues. For instance, France recently started applying DST in 2019 which leads to a 3% levy on revenue generated by tech giants and this led to a trade conflict with the United States because the latter accused the former of selectively targeting its technology firms[21]. The United States went to the extent of threatening to place sanctions on French products $2.4 billion in relation to what it termed the illogical unilateral imposition of taxes on digital companies[22]. Forums such as Amazon in Luxembourg being accused of receiving unfair state aid from Luxembourg through a favourable tax ruling. This case revolved around tax arrangements that allegedly allowed Amazon to pay significantly less tax compared to what other companies would under standard Luxembourg tax laws. The European Commission argued that this arrangement violated EU state aid rules by giving Amazon an unfair competitive advantage. progress even in larger formations such as the Eu[23].

The unilateral Digital Services Taxes (DSTs) implemented by countries such as France and Italy reveal the shortcomings of multilateral negotiations in the OECD-led process, as countries seek immediate remedies for actual or perceived revenue losses. Problems arise from these national taxes within international business and trade, research shows that DSTs may decrease global trade with global adoption without unanimous approval forming a world plan. But as acknowledged there are usually a trade-off between self-interests and common good which make achieving such coordination a strenuous exercise.

4. Statement on the Effects of National Policies on Global Reforms

The current global digital tax systems present similar challenges because they consist of numerous and diverse policies from various countries, each underpinned by a set of unique economic objectives and regulatory drivers. For instance, the European Union, has come up with the DST; yet internal tensions have prevented its actualization and increase in compliance costs for multinational digital companies navigating multiple jurisdictions[24]. However, some of the regional EU countries, such as Spain, Italy, and Austria, have their own unique DSTs, which have thereby created a fragmented legal environment that trading digital multinationals are forced to deal with[25].

[19] Felix Hugger, Ana Cinta Gonzalez Cabral, and Pierce O'Reilly, 'Effective tax rates of MNEs: New evidence on global low-taxed profit' (OECD, 2023) <4a494083-en.pdf> accessed 10 November 2024

[20] Neira Hajro, Kate Smaje, Benjamim Vieira and Rodney Zemmel, 'Digital resilience: Consumer survey finds ample scope for growth' (McKinsey Digital, October 2023) < Digital consumer survey finds growth opportunities | McKinsey> accessed 10 November 2024

[21] Wei Cui, 'The Digital Services Tax on the Verge of Implementation' (2019) 67(4) SSRN <ssrn-3510270.pdf> accessed 10 November 2024

[22] Sunita Doobay, Pamela A. Fuller, Henrique Lopes, Alexis Maguina, Robert J. Misey Jr., 'International Tax' 2024 54 Hein Online < International Tax> accessed 10 November 2024

[23] Pernilla Bergvad, 'Digital Services Tax - A feasible solution for Taxation of the Digital Economy?' (FACULTY OF LAW Lund University, 2020) < Färdig version Examensuppsats!> accessed 10 November 2024

[24] Charlotte McFaddin, 'Evaluating the Tax Veto in a Digital Age: Legislative Efficiency and National Sovereignty in the European Union' (SSRN, 2021) < ssrn-3800939 (1).pdf> accessed 10 November 2024

[25] Shannise Nomaqhawe Mbhele, 'An International Comparison of Digital Serving Tax' (University of Johannesburg, 2022) < Mbhele SN Wtm.pdf> accessed 10 November 2024

Some of the major effects of the various policies include the possibility of being charged levies twice. Multiple layers of tax will further create impedance, where companies operating in countries observing national DSTs and such prospective modified OECD regulations will be discouraged from investing heavily in the digital front.

It also destabilizes the long-term sustainability of multinational consensus projects such as the OECD's BEPS project. With countries focusing more and more on national interests, the possibility for a global taxation regime for the digital economy recedes further into the distance. Although such multilateral approaches still prevail as the ultimate goal, the examples of actions taken by the representatives of the major economies show the challenges of achieving the uniformity of digital tax policies adjusted to the differences in the member countries' economic profiles and public finance requirements. The OECD has reported that negotiations are at a stalemate, with over 60% of participants citing the inability to reconcile national fiscal needs with international agreements as a key barrier[26].

Findings/Results

Digital activities have led to massive changes in business activities from the traditional to the digital economy. Problems arise for governments trying to tax multinational corporations (MNCs). Traditional tax systems, which base people's taxation on physical location, are unable to properly capture firms whose core business model is international and are not relevant to the literature that seeks to solve problems defined and limited by physical structure. These dissimilarities have created revenue gaps that allow corporations to fully exploit globalization to minimize their taxes, thereby contributing to structural injustices in international taxation systems based on historical tax framework, which were originally designed for traditional functions rather than those of digital multinational corporations (MNCs). For instance, an OECD report revealed that digital MNC is able to set his effective tax rate at 9.5 percent while the average statutory corporate income tax rate in member countries stood at 23.2 percent[27]. Cognizant of the weaknesses of current tax regimes, many nations, especially in the EU, have addressed these problems through policies put in place by some countries and international organizations.

In response, several nations, particularly within the European Union, have implemented Digital Services Taxes (DSTs) which have been developed to justify that MNCs should have a proportional share of taxes in the jurisdictions where they obtain significant revenues although without a tangible presence. For example, 3% DST of France initiated in 2019 had collected €400 to €650 million within the first year of its implementation proving the revenues-generating effectiveness of the measures[28]. These taxes are chiefly intended to affect mostly big hi-tech firms that make enormous sales from internet advertising, stock dealing, and merchandise.

The unilateral approach to the adoption of DSTs may further disrupt the structure of international taxation, adding an extra burden to tax regimes for MNCs and increasing pressure in relations among trade partners. The problems arise due to the inconsistencies in the national tax policies that creates uncertainty and returns unproductive for MNCs who are compelled to operate in the midst of tangled legal requirements and possible exposure to tax double dipping. A 2022 study by the International Monetary Fund (IMF) reported that inconsistent national tax policies increase compliance costs for MNCs by an estimated 10% and expose firms to potential double taxation[29]. This fragmentation not only challenges basic tenets of a coherent international tax system but also poses the risk to jeopardize world trade by raising tensions in trade relations.

[26] Allison Christians, 'Taxation in a Time of Crisis: Policy Leadership from the OECD to the G20' (SSRN, 2010) < ssrn-1555799.pdf> accessed 10 November 2024

[27] Monica Gianni, 'OECD BEPS (In)Action 1: Factor Presence as a Solution to Tax Issues of the Digital Economy' (2018) 111 JSTOR < ssrn-3211971.pdf> accessed 10 November 2024

[28] Stefanie Geringer, 'National digital taxes – Lessons from Europe' 2021 35(1) South African Journal of Accounting Research <National digital taxes – Lessons from Europe> accessed 11 November 2024

[29] Fiscal Affairs Department, 'TECHNICAL ASSISTANCE REPORT-INTERNATIONAL TAXATION CHALLENGES AND OPTIONS' (IMF, 2023) <1GTMEA2023001.pdf> accessed 11 November 2024

The OECD's proposed global minimum tax rate of 15% aims to curb tax base erosion but faces implementation hurdles due to varying national priorities[30]. Nevertheless, achieving consensus remains a challenge when it comes to uniformity, especially when first-tier systems may have conflicting perceptions, most likely arising from differing influential economies on fair distribution. Hence, certain countries are eager to proceed with individual taxes, such as DSTs, to manage the static current-source imbalances and solve revenue needs. The long-term plan for integral international taxation still depends on the solutions to these complex coordination problems. There is potential for continued fragmentation if global consensus cannot be reached, risking the establishment of a new system of overlapping tax laws and additional trade quarrels. The pathway toward this also means that successful implementation must be backed by more diplomacy and honest conversations between nations, especially to avoid harm, through careful consideration of both developed and developing countries. The future of digital economy taxation combines these intricate factors with the imperative of trying to establish a fair and integrated system of international taxation that would suit the realities of the digital age.

Unilateral Measures v. Multilateral Cooperation

Considering the absence of a cohesive approach to taxing the digital economy, the adoption of numerous DSTs has been observed. One example is France's DST, which consists of a 3% tax on big digital companies that generate large revenues in France, targeting Google, Amazon, and Facebook, among others. Despite being used for a short time, the implementation of such taxes has fuelled bitterness, especially with the U.S., which claimed that DSTs impugn American enterprises. In response, the U.S. Trade Representative (USTR) acted and initiated investigations under Section 301 of the Trade Act of 1974, ultimately leading to threats of retaliatory tariffs on French imports[31]. This conflict raises the risks of ad hoc approaches leading to the fragmentation of the world's tax system, which, in turn, contributes to the disruption of global economic relations.

Self-generated DSTs also pose problems for businesses, which are confronted with different tax codes. While it is useful to comply with multiple, especially competing, tax regimes, they may stifle growth and innovation. Although the EU has called for a standardized digital tax regime within it, the aim is challenging to achieve because the countries have different motives. Thus, developing countries, which often depend on FDIs from digital powerhouses, are campaigning against such reforms for a similar reason: that they would decrease the appeal of their nations to MNCs. Such an imbalance underlines the need for attaining a multilateral solution that will enhance the fairness of distribution as well as promote economic incentives.

6. Challenges of Implementing a Global Minimum Tax

The OECD Pillar Two plan that seeks to establish a floor level rate of 15% applies a noble, if ambitious, attempt to curb tax competition by insisting that even MNCs in low-tax jurisdictions must pay taxes, to some extent[32]. This measure aims to eliminate the issue of profit switching in which MNCs book significant revenues in low-tax countries hence paying less tax. Even as it is backed by some of the world's highest-tax jurisdictions, the plan is strongly opposed by many low-tax countries such as Ireland, which competes for investment by offering low corporate tax rates. Profit shifting is the act of redistributing corporate income to countries with lower rates of taxation by MNCs. According to OECD, profit shifting reduces government revenues in the global sum of between $100 billion and $240 billion every year, or 4-10% of global corporate income tax revenues[33].

According to the International Monetary Fund (IMF) around 40% of MNCs profit is routed to tax havens each year and hence, creating a big tax base problem for countries which offer higher taxes. Implementation of the

[30] Simon Torkington, ‘What does the OECD global minimum tax mean for global cooperation?’ (World Economic Forum, February 2024) <A minimum tax rate of 15% on the profits of multinationals. | World Economic Forum> accessed 11 November 2024

[31] N Marques, PS Onge, G Campan, ‘Taxing the Tech Giants Why Canada Should Not Follow the French Example’ MEI < Taxing the Tech Giants – Why Canada Should Not Follow the French Example> accessed 11 November 2024

[32] Simon Torkington, ‘What does the OECD global minimum tax mean for global cooperation?’ (World Economic Forum, February 2024) <A minimum tax rate of 15% on the profits of multinationals. | World Economic Forum> accessed 11 November 2024

[33] Haiyan Xu, ‘The Reflection on the Magnitude and Disasters of BEPS Schemes’ (2019) 10(4) Beijing Law Review < The Reflection on the Magnitude and Disasters of BEPS Schemes> accessed 11 November 2024

global minimum tax concept comes with significant coordination issues, especially about international taxation and national dealing of tax authorities. There will be a requirement to characterize how nations would exchange and monitor tax information, data privacy, and data jurisdictions. However, the possibility of having loopholes or promoting regulatory evasion persisted. But to address these concerns, the OECD has come up with what is known as a "top-up" mechanism whereby a country can impose additional taxes on the basis that the effective tax rate of an MNC in a low tax jurisdiction is below the minimum standard set by the top-up tax[34]. However, there are some doubts as to how efficiently this system can be employed and what measures can be taken to ensure its compliance on the international level.

7. Political and Economic Implications of Reforms

The suggested changes that are part of Pillar One, which aims at the redistribution of taxing rights, are highly political and economic. Pillar One shifts tax rights from the residence country of the firm involved to the market jurisdiction, with a clear advantage to countries where digital services are consumed. Although the aim here is to solve the problem of stateless income—that is, income not subject to any tax at all—it causes developing nations to question whether or not they will get their equitable share of taxes. G20 developing economies have claimed that the allocation formula in the first pillar is unfair to them, as it only rewards large economies, and they should receive a bigger slice of the tax take because their consumers are more digitally active.

Such reform could result in conclusions that MNCs in the digitization technology sector would experience an increase in the tax levies they pay, thus affecting their profitability and business model. Google Ireland Ltd v. Revenue Commissioners describes how, for decades, the digital goliath managed its taxes in such a way that poses questions to other tax authorities around the world. If affected, these reforms would unbalance traditional tax planning, forcing companies to rethink their structures and possibly suffer a rise in overhead charges.

But those who emphasize the tax justice point of view claim that these changes are needed to fight the systemic unfairness in the existing global tax systems. Besides the proposed reallocation of taxing rights under Pillar One, it also tries to bring methodological changes with regard to taxing digital business while insisting on the need for international cooperation in addressing the problems of taxing cross-border activities. On the other hand, multinational corporations warn that such adjustments may result in them being paid for by consumers due to the end consumer bearing the tax cost. Such concerns raise important questions about how to achieve tax equity as well as economic stability, which remain at the heart of current global tax reform proposals.

When it comes to the outcomes of this research, one can underline the necessity of a higher level of cooperation at the international level in order to make the reforms of the tax system in the context of the digital economy both effective and fair. As the OECD's Base Erosion and Profit Shifting (BEPS) framework stands as one of the seminal blows in this field, much of its effectiveness will therefore depend on the capability of individual countries to balance national and global goals. The BEPS model itself has become threatened by the newest mutation of unilateral actions—digital services taxes (DSTs), which jeopardize both multilateral coordination and trade relations.

8. Relevance of Case Law in Tax Jurisdiction Disputes

It can be noted that case law offers valuable understanding of the issues arising in the field of taxing rights and jurisdiction in the context of the digital economy. Google Ireland Ltd. and Ireland's Revenue Commissioners' debate on jurisdiction over fees resulting from digital services in the EU is described in case C-193/18. The case put emphasis on some issues concerning the globalization of business and the use of the tax system in the attempt by firms to reduce their taxes in countries with high taxation rates[35]. While, after hearing and consulting the

[34] Prof.dr. M.F. (Maarten) de Wilde, 'Why Pillar Two Top-Up Taxation Requires Tax Treaty Modification' (SSRN, 2022) <ssrn-4018341.pdf> accessed 11 November 2024

[35] Charlie Taylor, 'Google Ireland agrees €345m tax settlement with Revenue' (The Irish Time, November 2021) < Google Ireland agrees €345m tax settlement with Revenue – The Irish Times> accessed 11 November 2024

interested parties, the ECJ found that Ireland could not apply the said withholding tax on the revenue derived by Google Ireland from the ad services, this case nonetheless reveals the challenges that individual jurisdictions face when it comes to applying their own tax laws to multinationals. This precedent once again emphasizes the need for an integrated global tax system since the uncoordinated movement in the form of unilateral measures may not address the issue of tax avoidance or profit shifting adequately.

Similarly, in the United States, the Wayfair v. South Dakota (2018) case brought the meaning of the nexus needed for state tax collection on remote sales to the Supreme Court[36]. This particular ruling eliminates the "physical presence" requirement for state taxation purposes and states that states can collect taxation money from out-of-state businesses due to economic and virtual nexus. We can see echoes of Wayfair all around us, especially as it relates to the taxation of the digital economy, because it highlights the need to introduce tax reforms in line with the present-day economy. The ruling means countries may explore similar systems to manage new transactions involving digital services, improving international tax cooperation by providing more comprehensible regulation of the digital economy.

9. BEPS and the Shift Toward Multilateral Solutions

A report by PwC (2023) on multinational taxation revealed that only 30% of countries have fully integrated the BEPS Pillar Two minimum tax rate 15% for domestic law, demonstrating slow and uneven progress[37]. Transfer pricing disputes remain over 50% of tax authorities surveyed indicating that transfer pricing audits are the primary focus of cross-border tax disputes. Pillar one and pillar two of the BEPS framework established by the OECD are oriented toward eradicating profit distribution and minimum income aspects while going beyond the state's interests. But as we have learned, the implementation of the above framework requires exceptional political will, accompanied by legal structures that ensure non-discriminatory procedures and equal enforcement. *Glencore International AG v. Commissioner of Taxation* (2020) in Australia is an excellent case explaining how difficult it is for countries to regulate and impose transfer pricing rules on multinational corporations. Here, the internal pricing structures of Glencore were accused of engaging in transactions that sought to reduce tax remittances[38]. The Australian Federal Court ruled in Glencore's favour on the grounds that it is challenging for the tax authorities to prove that pricing structures are unfair without general international benchmarks or international collaboration. Examples such as Glencore show that international regulation of profit splitting is necessary due to the ineffectiveness of attempts at the national level to counteract the aggressive behaviour of multinationals.

10. Unilateral Actions and Risks to Multilateral Cooperation

Several countries' adoption of DSTs beyond the OECD framework mirrors the increasing trend in protectionism and respective actions. These measures, meant to accord value generated within a country's economy, have been a shift from many countries that consider this value a tax discrimination scheme and contradictory to international trade rules. Like France, Italy and the UK imposed a 3% tax on revenues from digital services[39]. In the case, Apple Inc. v. Commission, by the European General Court, also set aside the decision of the European Commission to recover €13bn allegedly owed in unlawful state aid from Apple to Ireland[40]. The ruling also focused on the peculiarities of a single market member's tax measures within the common area, as well as a challenge that might result in a disruption of international standards. The case of Apple shows that trade tensions may be caused by unilateral actions that result in tax measures; everybody saw the Commission's action as an attempt to target

[36] Wayfair v. South Dakota (2018) 138 US 494 (US Supreme Court)

[37] Eur-Lex, 'Council Directive (EU) 2022/2523 of 14 December 2022 on ensuring a global minimum level of taxation for multinational enterprise groups and large-scale domestic groups in the Union' (European Union, 2022) <Directive - 2022/2523 - EN - EUR-Lex> accessed 11 November 2024

[38] Christian N Borg, 'Australian Transfer-Pricing in the Aftermath of Glencore Investment Pty Ltd v Commissioner of Taxation of the Commonwealth of Australia [2019]' 2022 29 Bond University < 33618-australian-transfer-pricing-in-the-aftermath-of-glencore-investment-pty-ltd-v-commissioner-of-taxation-of-the-commonwealth-of-australia-2019.pdf> accessed 11 November 2024

[39] N Marques, PS Onge, G Campan, 'Taxing the Tech Giants Why Canada Should Not Follow the French Example' MEI < Taxing the Tech Giants – Why Canada Should Not Follow the French Example> accessed 11 November 2024

[40] Stephen Daly, 'The €13bn question: is the fiscal State aid era over?' (SSRN, 2024) < ssrn-4808717.pdf> accessed 11 November 2024

American companies. It also points out that the use of unilateral DSTs is counterproductive since it triggers retaliatory tariffs and trade barriers, which hinder international trade. Pillar One would coordinate the taxing rights of countries and thus lessen the potential for legal disputes as well as countermeasures.

11. Capacity Building and Equitable Participation in Global Tax Reforms

A given country's capacity to participate in the formulation of new tax reforms is crucial to enhancing its ability to participate actively in the international tax reform process. There are often compelling logistical and capacity constraints that prevent a number of developing countries from unilaterally undertaking complex tax reforms; situations involving tax controversies within such countries are frequently manifested as issues related to the distribution of resources. For instance, in the case of Vodafone International Holdings BV v. Union of India (2012), the Indian Supreme Court ruled in favor of Vodafone and stated that India cannot tax an offshore transaction related to capital gains tax[41]. Aluminum from Novelis was being imported from the USA, and this complicated cross-border structure of the investment was beyond the understanding of the local tax department in developing countries. The structure of the article indicates that, with the help of capacity-building programs from the organization, developing countries can strengthen their rules and become engaged in the enforcement of effective worldwide tax reforms, including BEPS.

The Vodafone ruling also highlights that justice must be done in global tax legislation because developing countries have an inadequate legal framework to deal with the complex tax strategies adopted by large companies. Building these capacities will increase the ability of these countries to participate effectively in the OECD's work on base erosion and profit shifting and in shifting international taxing rights for large digital businesses.

Conclusion

The central focus of this article underscored that reforming corporate tax laws within the digital economy remains an intricate and pressing challenge for the global community. The expansion of digital enterprises and their new economic structures have exposed the limitations of traditional taxation systems, complicating the equitable taxation of cross-border digital transactions. The OECD's Base Erosion and Profit Shifting (BEPS) initiative has commendably laid a foundation for addressing these challenges, yet significant hurdles remain. The research has illustrated that political divergence, national interests, and the autonomous measures of individual countries hinder the establishment of consistent international standards.

The analysis of key legal cases highlights these complexities. For instance, of Google Ireland Ltd. v. Commissioners for HM Revenue and Customs[42], in which the UK court discussed the tax incidence of the revenues procured from the UK's digital advertising business but executed in Ireland. This case demonstrated the problem of applying conventional tax laws to multinational digital companies, in which profits are made in one country but taxed in another to take advantage of lower rates. The case also highlighted the ineffectiveness of current tax laws in controlling profit-shifting by digital giants, thus questioning the efficiency of the BEPS project agenda. This is in line with the general requirements for rules that reflect the value generated within market jurisdictions and correlate tax liabilities with these contributions.

Another remarkable case is the criminal proceedings – Amazon EU Sàrl v. Decision from the European Commission and Amazon, which claimed that the Grand Duchy of Luxembourg provided illegal state aid to Amazon, in the Ministère des Finances du Grand-Duché de Luxembourg[43]. Once again, the case illustrated the

[41] Y. Shiva Santosh Kumar, 'INDIA'S TAXATION REGIME: PERSPECTIVES ON THE PROPOSED CHANGES' (Manupatra, 2012) <INDIA'S TAXATION REGIME: PERSPECTIVES ON THE PROPOSED CHANGES> accessed 11 November 2024

[42] Charlie Taylor, 'Google Ireland agrees €345m tax settlement with Revenue' (The Irish Time, November 2021) < Google Ireland agrees €345m tax settlement with Revenue – The Irish Times> accessed 11 November 2024

[43] Charlie Taylor, 'Google Ireland agrees €345m tax settlement with Revenue' (The Irish Time, November 2021) < Google Ireland agrees €345m tax settlement with Revenue – The Irish Times> accessed 11 November 2024

problem of a bilateral or single-country solution to digital taxation. Amazon's tax avoidance scheme in Luxembourg exposed how large internet businesses could offshore their income and evade taxes in the real economy, thereby depriving the genuine economy of countries within the EU where the economic activities are mostly situated. This case reveals the exact rationale for having a set of rules across states, as differential treatment in fiscal laws allows corporate legal entities to manipulate jurisdictions for low taxation. It was while the EU was seeking to advance their agenda of using tax policies to fight unfair competition that the divergence of views between the U.S. and the EU became more explicit. In the perception of the latter, such actions singled out American companies for special treatment.

In the future, it should be required for global agencies and administrations to combine their efforts to develop efficient and non-discriminatory taxation policies for digital sales. As the cases above show, the legal framework in its current state, with no global regulation, results in diverse and unclear taxation systems that can open interstate tensions and loopholes for large MNCs to manipulate. Officials should rely more on bilateral and multilateral agreements than on exclusive actions that cause splits and instability in international taxation settings. The Inclusive Framework belonging to the OECD, which involves both developed and developing states, can be considered the most effective approach. However, a great deal of debate and fine-tuning of the concept is required for the OECD to encourage the participation of all global players in order to design a balanced strategy that fits the requirements of nations that may be in different phases of economic development.

This paper has, therefore, suggested that the OECD, working in conjunction with other international financial institutions and member countries, should continue to closely observe and assess the efficiency of these BEPS measures as they are disseminated internationally. This should be an ongoing process involving consultations with other major stakeholders such as large economies and emerging economies that might not have enough administrative power to enforce and implement a complicated digital tax framework on their own. In addition, this research recommends that the OECD employ existing legal decisions from the Google Ireland, Amazon EU Sàrl, and Dell Technologies cases for the purpose of determining the shortcomings and legal disputes that might be encountered under additional tax systems.

Thus, it can be claimed that only a united, comprehensive, and evolving strategy can lead to a reasonable and equitable taxation of the digital economy. The initiatives of the OECD remain laudable, but they will only achieve the intended results if fostered by international support that targets various digital-specific concerns highlighted in this study. It is hereby notably recommended that countries must avoid unilaterally imposing digital tax measures, as doing so would trigger legal actions and induce a structure of burdensome cross obligations that negate the purpose of tax reform. On the other hand, by promoting multilateral consensus, global society can guarantee that digital corporations pay their fair share while maintaining the beneficial flow of international trade and knowledge creation.

NOTES:

60

jims
JIMS Engineering Management Technical Campus

Printed, Published and owned by Amit Gupta. Printed at Shubham Enterprises, 129, DSIDC Sheds, Okhla Indl. Area, Phase-I, New Delhi - 110020.
Published at JIMS Engineering Management Technical Campus 48/4, Knowledge Park-III, Greater Noida. Editor: Amit Gupta