

# Study on Evolution of White Collar Crimes in the Digital Age

**Amitesh Milind Kamble**

LLM (Criminal Law) 1st Year 2nd Semester

School of Law, Sandip University, Nashik, Maharashtra, India

**Abstract:** *This paper intends to investigate the occurrence of white collar crime in India, its development over time, and its effects on the economy and society. White collar crime refers to financially motivated, nonviolent offenses committed by those in positions of power or trust. While it has always been present in India, there has been a significant rise in recent years, resulting in substantial economic losses and damage to public confidence. Through a review of literature and data analysis, this study aims to comprehend the factors contributing to the escalation of white-collar crime, its impact on the Indian economy, and its consequences for society. The research also suggests potential solutions to combat this type of crime and promote ethical business practices.*

**Keywords:** White-Collar, Digital Age, Criminal Law, Economy

## I. INTRODUCTION

White collar crime, a term first coined by sociologist Edwin Sutherland in 1939, refers to non-violent, financially motivated crimes typically committed by individuals, businesses, or government officials in positions of trust and authority. These crimes often involve deception, fraud, and manipulation, and they have traditionally been associated with boardrooms, financial institutions, and government offices. In India, white collar crime has manifested in various forms, including corporate fraud, embezzlement, and money laundering. In the modern world, the concept of white-collar crime has not only retained its relevance but has also undergone a profound transformation. According to data from the Reserve Bank of India (RBI), digital transactions in India have been surging, with a substantial increase in digital payments, internet banking, and mobile wallet usage.

In 2020, digital payments grew by 25.2% in terms of volume and 43.4% in terms of value compared to the previous year. This growth in digitalization and financial technology has introduced a new paradigm in the realm of white-collar crime. White collar crime has been a prominent problem in India for numerous years, with its various forms constantly changing and affecting society in different ways. From bribery to deception, these unlawful acts have not only impacted individuals, but also have significant repercussions on businesses and the overall economy.

In order to fully understand the extent and consequences of white-collar crime in India, a comprehensive research approach must be utilized, incorporating both qualitative and quantitative methods of data collection. In this paper, we will delve into the development of white-collar crime in India and analyse its effects on society from a theoretical standpoint. Furthermore, we will investigate the different research techniques employed to examine this subject, ultimately addressing the inquiry: what is the true nature of white collar crime in India? Furthermore, we will explore technological solutions and cooperation between various stakeholders, such as law enforcement agencies, the private sector, and international entities, to combat cross-border digital crimes effectively. Hirsch and Gottfredson (1987)<sup>1</sup> explained white collar crime unlike other common crime, the reason they contravention of the law is not similar with normal crime". Cubicle wrongdoing was characterized by Edwin Sutherland as a "wrongdoing carried out by a man of respectability and high economic wellbeing over the span of his occupation."<sup>2</sup>

### Meaning of white-collar crime in digital age

White-collar crime is a type of crime committed by persons from upper-class backgrounds who are members of a recognized social group. These crimes are perpetrated as a result of their employment.

People that perpetrate this crime often have a superior awareness of the people they are working with, technology, their area, disciplines, and so on.

White-collar crime has developed dramatically over time. These crimes are committed in massive organizations that engage in a variety of activities. These crimes are typically committed in industries such as trade, business, health, education, and a variety of other huge organizations.

## **II. EVOLUTION OVER TIME**

Over time, there have been significant changes in the landscape of white-collar crimes in India. While traditional forms like bribery and embezzlement still exist, newer and more complex forms such as cybercrime and money laundering have emerged, posing a threat to the stability of the country's financial system. The Indian criminal code, which was first established and defined in 1860, covers a wide range of white-collar offenses and outlines the corresponding penalties for each. These include acts involving the concealment or deception of assets, fraudulent activities committed by public servants or bankers, and other breaches of trust. In recent years, the rise of technology has brought about a surge in cybercrimes, including the hacking of computer systems to obtain sensitive information or carry out financial frauds. Therefore, it is crucial for both individuals and businesses to stay informed about these evolving forms of white-collar crime and take necessary measures to safeguard themselves from becoming victims. The individuals who commit these offenses often possess advanced knowledge in areas such as finance management, engineering, medicine, organizational theory, and information technology<sup>3</sup>. When studying criminology at the college level, students gain insight into the complexities of white-collar crime and its impact on society. This subject requires a critical and analytical approach to comprehend the motives behind these violations and their repercussions on both individuals and institutions. The study of white-collar crime allows us to safeguard ourselves against these crimes and hold those responsible accountable for their actions. As stated by (Maity), white collar crime often takes place within large and intricate organizations, emphasizing the importance of acquiring a comprehensive understanding of this subject to prevent future occurrences.<sup>4</sup>

## **III. INCREASE IN WHITE COLLAR CRIMES IN INDIA**

India has a very evident economical divide between its social classes, rich and poor. There is a huge chunk of population that is uneducated and is below poverty line that causes lack of awareness and being more susceptible to white-collar crimes. In addition to this, lack of proper implementation of laws and personal factors like greed and competition among peers are some factors involved.

Some of the many reasons augmenting the growth of white-collar crimes in India are explained below:

- **Lack of Strict Laws:** Though India already has laws against financial fraudulence, these need to be made more stringent to penalize offenders. Perpetrators tend to exploit loopholes in the existing laws and getaway successfully.
- **Greed:** It is believed that there is greed inbuilt in the nature of man. It states true in the cases of white-collar crimes as these are mostly committed by people already part of high society circles with so much wealth that already cannot be accounted for.
- **Lack of Awareness among General Population:** People who fall prey to white-collar crimes often fail to make sense of the nature of the crime that has been committed and are unaware of the procedures to be followed in order to register a complaint against such offence.

## **IV. TYPES OF WHITE-COLLAR CRIMES**

Types of white-collar crime in digital age:

There are many cybercrimes which are governed under cyber law that have emerged or evolve due to digitalization

### **Identity Theft:**

- **Description:** Identity theft involves stealing personal information to commit fraud, such as opening credit cards or filing taxes in someone else's name.
- **Examples:** The Equifax data breach in 2017 exposed the personal data of over 143 million individuals.

- Statistics: Identity theft cases have been on the rise, with millions of reported incidents annually.

#### **Online Scams:**

- Description: Online scams come in various forms, from fake online marketplaces to advance-fee fraud.
- Examples: Ponzi schemes like the case of Bernie Madoff, who defrauded investors of billions through digital records and communication.
- Statistics: The Federal Trade Commission (FTC) receives millions of complaints about online scams each year.

#### **Insider Trading:**

- Description: Insider trading involves using non-public information to make stock trades for personal gain.
- Examples: Cases like the 204 cases of Matthew Martoma, who used insider information from clinical drug trials for illicit stock trading.
- Statistics: The SEC continues to investigate and prosecute insider trading cases involving digital communication.

#### **Money Laundering:**

- Description: Money laundering is the process of disguising the origins of illegally obtained funds.
- Examples: Cases involving digital currencies like Bitcoin have emerged, making tracking money laundering more challenging.
- Statistics: The Financial Action Task Force (FATF) continues to address money laundering risks in the digital era.
- Digital white-collar crime, with its intricate web of factors and vulnerabilities, has become a growing concern in the digital age. Criminals are continually finding new ways to exploit digital platforms and systems for their gain, while the challenges faced by law enforcement and cybersecurity experts continue to evolve. Let's delve into this issue with more detail, supported by research and real-time statistics.

### **V. FACTORS FACILITATING DIGITAL WHITE-COLLAR CRIME**

- Anonymity: One of the most attractive aspects of the digital realm for criminals is the cloak of anonymity it provides. The ability to operate behind pseudonyms or untraceable digital footprints makes it exceptionally challenging for law enforcement to identify and apprehend wrongdoers. A study by the University of Twente in the Netherlands found that cybercriminals often use a multitude of techniques to obfuscate their identities, such as VPNs and Tor networks, making it difficult to track them.
- Global Reach: The internet's global nature allows criminals to target victims and collaborators worldwide. According to a report by Europol, this global reach enables various types of digital crime, from fraud to cyberattacks, to affect individuals and organizations on a global scale.
- Automation: Criminals harness the power of automation to streamline their operations. This includes using bots for social engineering attacks, mass spamming, or conducting automated reconnaissance. Research from cybersecurity firm McAfee highlights the increasing sophistication of automated tools used by cybercriminals, allowing for large-scale, efficient attacks.
- Accessibility: Digital platforms are easily accessible to virtually anyone. This accessibility means that both seasoned cybercriminals and inexperienced individuals can enter the world of digital crime. The growth of underground forums and marketplaces on the dark web provides resources and knowledge for aspiring criminals.

### **VI. CHALLENGES IN DETECTING AND PREVENTING DIGITAL WHITE-COLLAR CRIME**

- Detecting and preventing digital white-collar crime presents significant challenges for law enforcement agencies worldwide: These crimes encompass a range of illicit activities conducted through digital means, such as fraud, embezzlement, identity theft, and cyberattacks. Here, we'll delve into the complexities involved in addressing this issue and the jurisdictional hurdles that often arise.

- **Sophistication of Perpetrators:** Digital white-collar criminals are often highly skilled and technologically savvy. They employ sophisticated techniques to cover their tracks, making it difficult for investigators to trace the origins of the crimes.
- **Cross-Border Nature:** Many digital crimes have a transnational dimension, where perpetrators can be located in one country, victims in another, and infrastructure (e.g., servers) in yet another. This creates a complex web of jurisdictions that need to cooperate.
- **Jurisdictional Challenges:** When a crime involves multiple countries, determining which nation has the authority to investigate and prosecute can be perplexing. Extradition laws, differing legal systems, and the absence of international cybercrime regulations further complicate matters.
- **Rapid Technological Advancements:** The ever-evolving technology landscape provides criminals with new tools and tactics, while law enforcement struggles to keep pace with these changes.
- **Resource Constraints:** Many law enforcement agencies face resource limitations, including budget constraints and a shortage of skilled cybercrime investigators. This hampers their ability to effectively combat digital white-collar crime.
- **Evidence Collection:** Gathering digital evidence that can stand up in court is intricate. The digital trail can be easily manipulated or erased, making it vital to preserve evidence accurately.
- **Public Awareness:** Many individuals and businesses are unaware of the risks they face from digital white-collar crime, which can lead to insufficient preventative measures and reporting when they fall victim to such crimes.
- **Cooperation and Legal Frameworks:** International cooperation and the establishment of robust legal frameworks for dealing with cross-border digital crimes are essential but challenging to implement

## **VII. REGULATORY AND LEGAL RESPONSES**

In India, digital white-collar crime is governed by the Information Technology Act, 2000 (IT Act) and the Indian Penal Code (IPC). Key provisions include:

### **Information Technology Act, 2000:**

- Section 43: Penalties for unauthorized access and damage to computer systems and data.
- Section 66: Punishment for computer-related offenses and unauthorized access.
- Section 66C and 66D: Dealing with identity theft and cheating by personation.
- Section 66E: Violation of privacy by capturing and transmitting private images.
- Section 67: Addressing obscene material in electronic form.

### **Indian Penal Code (IPC):**

- Section 420: Pertaining to cheating and inducing property delivery.
- Sections 463 and 464: Making and possessing counterfeit electronic records.
- Sections 468 and 469: Dealing with forgery for cheating and its punishment.
- Section 47: Use of a forged document as genuine.
- Section 509: Addressing acts intended to insult the modesty of a woman.

## **VIII. FINDING OR RESULTS<sup>5</sup>**

To prevent the White Collar Crimes in India we have to initiate some ways.

- **Data Analytics and AI:** Leveraging advanced data analytics and artificial intelligence (AI) technologies are paramount in detecting fraudulent activities.
- **Employee Education and Training:** Educating employees about the nuances of white-collar crimes and common fraud tactics is a foundational step.
- **Internal Controls and Audits:** Implementing stringent internal controls, coupled with regular audits, ensures transparent financial practices.

- Regulatory Compliance: Staying up-to-date with new regulatory activities and compliance standards are vital. Compliance not only mitigates legal risks but also nurtures an environment of accountability, deterring both internal and external fraudulent activities.

### CASE LAWS

Abhay Singh Chautala v. C.B.I.

There were two appellants in the present case against whom a charge sheet was filed for committing an offence under Section 13(1)(e) and 13(2) of the Prevention of Corruption Act, 1988 read with Section 109 of the Indian Penal Code, 1860 in separate trials. It was alleged that both the accused had accumulated disproportionate wealth as per their income when they were they members of the Legislative Assembly.

When the Central Bureau of Investigation (CBI) initiated its investigation, it was found that the father of the appellant had acquired huge properties and same as the case with the appellants. The High Court held that the appellant had provided a totally different office(s) of the accused than they were actually holding at that time. Thus, the sanction under Section 19 of the Prevention of Corruption Act, 1988 was held to be without any merit.

### IX. CONCLUSION

White-collar crimes have become a significant problem in India, and they have a detrimental impact on the country's economy and development. The government and regulatory bodies need to take proactive measures to prevent these crimes and prosecute those responsible for committing them.

Strengthening the legal system, improving the regulatory framework, increasing awareness, and implementing whistleblower protection are some of the steps that can be taken to prevent white-collar crimes in India and create a more transparent and accountable business environment. It is important to note that preventing white-collar crimes requires a coordinated effort from all stakeholders, including the government, regulatory bodies, businesses, and the public.

### REFERENCES

- [1]. The Transformation of Crime in the Information Age (Crime and Society) by David S Wall.
- [2]. White Collar Crime and Corporate Crime, By Kanan Bhardwaj.
- [3]. White Collar Crimes by Shailesh Kumar Singh.
- [4]. White Collar Crimes [Indian and Abroad] by Dr. Manju Koolwal.
- [5]. [https://www.researchgate.net/publication/349134240\\_White-Collar\\_Cybercrime\\_Evaluating\\_the\\_Redefinition\\_of\\_a\\_Criminological\\_Artifact](https://www.researchgate.net/publication/349134240_White-Collar_Cybercrime_Evaluating_the_Redefinition_of_a_Criminological_Artifact)
- [6]. [https://www.researchgate.net/publication/357835747\\_White\\_Collar\\_Crime\\_in\\_Indian\\_Context](https://www.researchgate.net/publication/357835747_White_Collar_Crime_in_Indian_Context)
- [7]. <https://www.legalserviceindia.com/legal/article-10873-white-collar-crimes-in-india.html#:~:text=Conclusion%3A,those%20responsible%20for%20committing%20them.>