WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Digital Vigilance: The Role of Technology and E-Governance in Strengthening India's Anti-Corruption Laws

Siddharth Pundir* *and Sachin Kumar*****

Law College Dehradun, Uttaranchal University

ABSTRACT :

Corruption has always been a menace to the democratic integrity and growth of social economy, in India. From systemic weaknesses in detection, enforcement, and prevention, technology and e-governance could have heralded a new era in combating corruption. Enforcement authorities with a digital avatar in disguise are using , in a very sophisticated manner, technologies like AI, Blockchain, Data Analytics, and Machine Learning to es identify, complex pattern of financial frauds over gigantic data sets and prosecute the criminals. In order to give the legal basis for obtaining and using digital evidence with minimum procedural delays, legislation has been passed such as the Prevention of Corruption Act, 1988 (as amended), Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, and Bharatiya Nagarik Suraksha Sanhita, 2023. Some e-Governance projects aiming to reduce discretion and thereby scope for bribery include Direct Benefit Transfer, Government e-Marketplace, Bhoomi Project, and digital whistleblower portals. The Constitution and several Supreme Court decisions of India bind the courts to harsh answers laid down on electronic evidence, in particular section 65B of the Indian Evidence Act. With these powers, the concept of corruption, too, has evolved and has thus become a foremost priority to update framework reforms on legal, techno-logical, and institutional aspects at regular intervals. Equally, citizen involvement aided by inter-agency coordination would act as an equilibrating force on tech-enabled anti-corruption scenery, providing visibility and accountability in the governance system-the maintenance of trust with the public will thus be ensured.

Keywords: Digital Vigilance, E-Governance, Prevention of Corruption Act, Artificial Intelligence, Blockchain, Data Analytics, Bharatiya Nagarik Suraksha Sanhita, Electronic Evidence

Introduction

Corruption stands as the greatest ailment that Indian democracy suffers and breeds socio-economic disparity. Yet many theories of corruption still face challenges to their enforcement. Methods and technologies for detection, investigation, and prosecution have remained unchanged and thus have no answers to the contemporary manifestations of corruption. Hence, this implies technology and e-Governance as heavy vehicles supporting a framework of anticorruption measures based on transparency. Digital Vigilance uses technology, innovation, and platforms to redesign the entire chain of action for the detection, prevention, and deterrence of corruption, enabling citizens and institutions to hold the corrupt accountable.[1]

Definition of Digital Vigilance and E-Governance in the Context of Anti-Corruption

Corruption is perhaps the worst affliction for Indian democracy and has been a source of socio-economic disparity. Yet other areas of corruption theories are still enforcing problems. Detection, investigation, and prosecution methods and technologies have not followed the recent faces of corruption. Hence technology and e-governance will act heavy-duty vehicles to the legal regime of an anti-corruption agenda based on transparency. Digital Vigilance shall stand for a new concept wherein technology, innovation, and platforms shall be used to restructure end to end all action chains for detection, prevention, and deterrence of corruption and also to empower citizens and institutions to seek redress and hold the guilty accountable.

Importance of Technology in Combating Corruption in India

Political corruption is an evil that slime incurred in Indian democracy and sets the manner for social and economic inequalities. But surely to name a few anti-corruption laws, each would somehow answer against the effectiveness of implementation. The older classical methods and technologies of detection, investigation, and prosecution have not kept pace with new faces of corruption. Therefore, technology and e-Governance must become a strong means for strengthening the legal framework for an anticorruption agenda of transparency. Digital vigilance is the digital-redesign of the entire corruption-action

---

[*] Student, B.A. LL.B. (Hons.), Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

[**] Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

[1] Rajesh Kumar, "E – Governance as an Anti – Corruption Tool in India: An Analysis", 1 *IJSSRR* 71 (2023).

chain: detection, prevention, and deterrence, using technology, innovations, and platforms to empower citizens and institutions to hold corrupt persons accountable.

Emergence of Technology and E-Governance in Indian Administration

Certain levels of corruption, in the process, actually undermine a few of the principles of Indian democracy, and in conjunction with these, cause a range of socioeconomic disruptions. While the country has laws regarding corruption, their implementation had always been sharply criticized. Corruption has morphed like a mercury through the ages, and anti-corruption had seldom been able to keep pace with the changes in any of their investigation, detection, or prosecution facets. Therefore, an anti-corruption agency should identify technology and E-governance as the essential pillars of safeguarding legal recourse towards transparency. Digital vigilance tries to create new methodologies for the detection, design, prevention, and deterrence of corruption through technology, innovation, and platforms being able to trust citizens and institutions for accountability.[2]

Once so perceived, corruption has been at the center-stage as the chief malaise for democracy and socio-economic development. There being the myriad of legal remedies under the erstwhile constitution said to target the corruption, inadequacy had always arisen when it came to the practical level of enforcement. The methods of detection, investigation, and prosecution practiced practically by every anticorruption agency in the country today cannot possibly keep up with the metamorphosis of corruption across the world. In this backdrop, it seemed that technology and e-governance measures provide for some untapped potential with the anti-corruption setup and hence against transparency in India. Digital vigilance, the wave of technological innovations and ferry them through corruption detection, prevention, or deterrence, thereby empowering citizens and institutions alike to make each other accountable.

Corruption was, is, and always will be considered the greatest threat to democracy and socio-economic development. Constitutionally, there should be an exhaustive legal machinery to operate on the issue of corruption, but its enforcement has been wanting. Outdated and ill-designed methods of detection, investigation, and prosecution seem to be unable to keep pace with the dynamic metamorphosis of corruption. Against this background, technology measures and e-governance theoretically enhance the anti-corruption framework and transparency in India. Digital vigilance open the doors for technological innovations and transport themselves into new realms of corruption detection, prevention, and deterrence. From within, they prove to be the agents of citizenry and institution empowerment, holding each other accountable.

Such corruption hindrances are alleged to cause a major distortion to socio-economic growth on account of resource diversion and erosion of public trust in institutions. Anti-corruption roadblocks such as individual audits, physical inspections, and whistleblower mechanisms could almost always fail-there might be human error, bias, or untimeliness. Maybe technology, in this regard, has the scope to compensate for most of this. The automated government service delivery system takes away discretionary power from public agents-these cases are rule-based and electronically monitored. With this, the Direct Benefit Transfer (DBT) has done much for closing the leakages in the welfare schemes wherein subsidies are directly transferred into the bank accounts of rightful beneficiaries, as also reinforced under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, while the e-procurement and e-tendering platforms have ensured transparency in government contracts by publishing the whole bidding process and the decisions online to map any irregularities under the General Financial Rules, 2017. In principle, this might enrich transparency for literally anyone to scan all steps of the process. It thereby seals the time-lag that occurs during the identification and obliteration of any deviation from the standards, wherein no single step of corrupt practice can go unobserved. The technology mentioned above thus assists to metamorphose governance into a culture of transparent and mustered accountability; any other time, it would be outlandish.[3]

Legal Framework

Anticorruption law acts as a generic title to a series of laws to address various aspects of corruption. In other words, there is dual criminal liability under the anticorruption law; both the giver and the taker of the bribe are punishable under it. Standing at the center of this double system is the Prevention of Corruption Act, 1988 (hereafter 'PCA'), being the primary statute in relation to corruption offenses in public offices. It is secondarily supported by statutes such as the Lokpal and Lokayuktas Act, 2013, for creating institutions aimed at secondary anti-corruption objectives, the Benami Transactions (Prohibition) Act, 1988, for exterminating illegal wealth concealment, the Prevention of Money Laundering Act, 2002, for tackling money laundering arising from corruption, as well as some sections of the Indian Penal Code, 1860 (of which a majority have now been replaced by the Bharatiya Nyaya Sanhita). All these operate parallelly with each other, population onto one side of the corruption spectrum- detection, defense, and prosecution-with the Constitution duly brought onto the scene every time-inclusive of due process, presumption of innocence, and so forth.

Prevention of Corruption Act, 1988 (PCA)

In India, the various anticorruption laws combine to form an entire system to check corruption by carrying out one or the other mode of procedure concerning the persons or institutions. Dual criminal liability means that the person offering the bribe and the person accepting it are liable and punishable under the law. At the center stage of this double system is the "Prevention of Corruption Act, 1988 (hereafter PCA)".Which is basically the central legislation relating to offences of corruption by persons in public offices. Secondly, and supporting these courts come statutes such as the Lokpal and Lokayuktas Act, 2013, which set up bodies for secondary anti-corruption purposes; Benami Transactions (Prohibition) Act, 1988, which deals with the concealment of illegal wealth through property transactions; Prevention of Money Laundering Act, 2002, which looks at laundering proceeds of corruption; and certain provisions of the Indian Penal Code, 1860, although most of these have been replaced by the Bharatiya Nyaya Sanhita. These

[2] P. Fusco, E. Nazzarro, et.al., "Fascial Plane Block and ERAS: It's Time to Drug Sparing", 1 *JCA* 112 (2024).

[3] P.K. Mohanty, "Using e-Tools for Good Governance & Administrative Reforms", available at: https://www.cgg.gov.in/wp-content/uploads/2017/07/eGovPaperARC.pdf (Visited on March 5, 2025).

statutes work concurrently with each other and with each statute focusing its attack on some facet of corruption-detection, prevention, and punishment-with the constitution duly reminded and observed on every occasion as to due process, presumption of innocence, and so forth.[4]

Amendments

Amendments within a 1988 act, principally the "Prevention of Corruption Act", are thus largely important within the construct of the anti-corruption legal framework in India, given that they catapulted the law closer to compliance with the standards prescribed under the United Nations Convention against Corruption (UNCAC). Far-reaching developments include insertion of criminal liability for bribe giving into section 8 of the PCA, 1988, thereby imputing responsibility not only on the public official who receives the bribe but also upon the private person or corporate body who offers the undue advantage in private business. This wide-ranging liability panorama may thus close a few loopholes through which the giver of the bribe would quite often escape prosecution, thus increasing the deterrence factor under penal provisions.

From this stand, the other two amendments make criminal liabilities binding upon corporate entities: "Having found that legal persons, companies, partnerships and other legal entities may be used to facilitate corruption", Section 9 of the PCA, 1988 duly amended, places liability on commercial organizations in respect of corruption arising out of administrative acts; that is, as to whether in the course of such acts they failed to prevent any person associated with such organization from corruptly obtaining, or attempting to obtain, either for business opportunity or for advantage, any business opportunity or advantage. With such incentives existing in the law, companies would be inclined to put in place internal compliance programs that would ensure that their business is conducted in an appropriate way. "So, in layman's terms, the PCA is basically an anti-corruption law, criminally punishing every natural and juridical person. Thus, to combat corruption through organizational governance mechanisms and culture besides the conduct of an individual implied in the legislation. So, this amendment speaks volumes: India has so far fortified its anti-corruption architecture in an all-encompassing consumptive approach to those posed by corruption in public and private life-UNCAC Style.[5]

Other Relevant Laws

The Whistleblower Protection Act (2014) is the principal piece of legislation that confers legal protection upon those persons who disclose corruption in public or private institutions. It considers these persons to be in peril, and therefore offers a framework to protect their interests against retaliatory action or victimization or intimidation or harassment on any such grounds. Digital workers can be a great value option under the Act insofar as permitting complainants to lodge complaints digitally against anybody anonymously via secure online portals; to track digitally the progress of investigations; and to share evidence and information securely with the concerned authorities. This would make reporting easier without compromising on the forensic quality of evidence, allow evidence to be secured with administrative speed, and thereby considerably ease either completely or partially the efficient functioning of the Whistleblower Protection mechanism.

Information Technology Act, 2000

Opened in 2000, the Information Technology Act sought to offer an enabling framework in India for e-commerce and communications. The Law recognizes, among other things, electronic records and digital signatures, which courts in India may accept under Section 4 as evidence. Since under Section 2(1)(t), electronic records may comprise data, image, sound, or any other form of information generated, sent, received, or stored in digital form, keeping such records will consider the option of government departments and public offices over any scope of manipulation or destruction under physical paper records that have often been used as a medium by corrupt officials.

Having come into force in 2000, the Information Technology Act was intended to create an enabling framework for electronic commerce and communications in India. The Law recognizes electronic records and digital signatures, inter alia, which shall be accepted in evidence by the Indian courts under section 4. Since electronic record shall include data, image, sound, or any other form of information generated, sent, received, or stored in digital form as per Section 2(1)(t), the recognition of digital records has empowered government departments and public offices to keep records of their transactions, contracts, and decisions with only the least scope for manipulation or destruction that has been exercised on paper records in aid of corrupt officials.[6]

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, appears to be an effort by India to draft legislation to control the complex issues of data protection and privacy in this modern technological age. Paramount importance being given to the treatment of personal data has thrown in some kind of interference in an investigation into corruption relating to collection and handling of digital evidence. A data fiduciary is, under Section 17 of the Digital Personal Data Protection Act, 2023, obligated to report any breach of data that compromises personal data's confidentiality and integrity to the Data Protection Board as well as notify immediately of breaches that affect significant digital evidence in corrupt recording.

---

[4] Irshad Khan, Muzammil Haider, et.al., "E-Governance in India and Its Role in Modern Governance: A Conceptual Overview", 10 *IJRTI* 163 (2025).

[5] Le Thanh Ha, Thanh Trung To, et.al., "The Roles of E-Government in Combating Corruption: Evidence from European Countries", 1 *JSTPM* 225 (2024).

[6] S. Sri Sakuntala, Srinivas Sarakanam, et.al., "The Complexity of Corruption and Recent Trends in Information Technology for Combating Corruption in India", 27 *PAP* 193 (2024).

Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)

The "Bharatiya Nagarik Suraksha Sanhita, 2023" (BNSS), effective from the 1st of July, 2024, stands as an important reform query criminal procedural law in India and finds several provisions to weave digital processes into the criminal justice system. These reforms pertain to anti-corruption enforcement to make legal processes more efficient, transparent, and integral. Digitization, under BNSS, is interwoven with criminal investigation, prosecution, and adjudication procedures and processes. These provisions work against corruption by eliminating delays and discretion and resisting tampering or destruction of evidence.

Coming into force from the 1st of July, 2024, "The Bharatiya Nagarik Suraksha Sanhita, 2023" (BNSS) marks a landmark reform in Indian criminal procedural law, with wide provisions for the insertion of digital processes into the administration of criminal justice. Now, the enforcement against corruption would undergo these reforms to seek further efficiency, transparency, and integrity in legal processes. Digital technology is being used for every aspect of criminal investigations, prosecutions, and adjudications under the BNSS. These measures against corruption are intended to sustain the elimination of delays or human discretion and protect evidence from being tampered with or destroyed. The enactment of the "Bharatiya Nagarik Suraksha Sanhita, 2023" (BNSS), which came into force from July 1, 2024, is the landmark criminal reform introduced into Indian procedural law, in relation to wide provisions for insertion of digital processes in the administration of criminal justice. Thus, enforcement against corruption stands to gain from these reforms to bring in more efficiency, transparency, and integrity into legal processes. Now by these digital means, all the phases of criminal investigation, prosecution, and adjudication become digitized as per BNSS. Such an initiative fights corruption by removing delay, reducing human discretion, and preventing the tampering or destruction of evidence. One of the foremost features of BNSS is an FIR registration under Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023, through electronic means. It allows the complaint to file their FIRs online without having to visit police stations physically. Keeping in view intimidation and coercion often practiced in corruption-related cases, a citizen or whistleblower can safely and in good conscience report corruption through electronic means of registering an FIR. The fast and traceable registration of a complaint under this provision would allow the investigation into corruption to proceed swiftly while preserving the freshness of the evidence, which is a crucial factor in making successful prosecutions.[7]

FIR filing by electronic means: This is a case of a prohibition under the BNSS. Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023, provides for the registration of First Information Reports (FIRs) for crimes via electronic means. The very proviso allows complainants to lodge the FIR at their homes through some digital platform and hence are not bound to go to police stations vis-a-vis the complainants' physical presence being considered. Mostly, issues of corruption entail intimidation or coercion for complainants; hence, giving back power to citizens and whistle-blowers through the electronic system of FIRs is a way to report acts of corruption safely and securely. It aids in quick and traceable complaint registration so that investigation into corruption may be immediately started, along with the freshness of evidence preserved, thus increasing the potential for successful prosecution.

Filing of FIRs through electronic means: This is a prohibitive norm under the BNSS. Section 173 of the Bharatiya Nagarik Suraksha Sanhita, 2023, conditionally allows the case of crimes to be registered by electronic means. Thus, the proviso makes it possible for complainants to lodge FIRs from their homes through digital platforms as compared to being forced to appear in person at the police station for the lodging of FIRs. Mostly, corruption cases involve intimidation or coercion of the complainants, so the electronic system of FIRs returns power to the citizens and whistle-blowers to report acts of corruption safely and securely. It helps in the speedy traceable registration of complaints, so that investigations into corruption can be started immediately while the evidence is still fresh and thereby increasing the likelihood of the successful prosecution of the case.

The procedural safeguard of search operations has been further amplified to protect the audiovisual recording of search operations by investigative agencies as one potentially mandatory recording under "Section 100 of the Bharatiya Nagarik Suraksha Sanhita, 2023." In corruption cases, the search is an important stage for collecting incriminating evidence of illegal money, unauthorized documents, and digital devices aimed at overriding incriminating information. Therefore, compulsory audiovisual recording of the search will compel the search to be conducted in the public eye and thereby will dissuade any undue interference by any law enforcement agency against the accused. The audio visually recorded search procedure would hence be admissible as evidence and addition to the credibility of the investigative mechanism, thereby protecting both investigators and the suspects from being wrongfully accused.[8]

The BNSS has touted in the creation of "Section 532 of the Bharatiya Nagarik Suraksha Sanhita, 2023", allowing proceedings to be held electronically. Physical proceedings would entail a heavier expense and would present logistical difficulties if an electronic trial premise is made. Such electronic trials, indeed, help in trying high-profile corruption cases wherein security issues interfere with the usual processes of the court or intimidate witnesses or create geographical interference. It makes the judiciary stand benefitted by way of the presentation of digital evidence in a secured manner as against the protection of the witnesses/complainants who would otherwise be in fear of retaliation.

BNSS has taken a phenomenal initiative by drafting "Section 532 of the Bharatiya Nagarik Suraksha Sanhita, 2023", that permits electronic hearings. Physical hearings are more expensive to conduct and logistically unfriendly when the trials are being pursued virtually. These electronic trials could be used in high-profile corruption cases where security considerations would interfere with the court proceedings as ordinarily conceptualized or where intimidation might take place against witnesses or geography might conflict. This will reduce the undue delays in effective judiciary by facilitating secure presentation of digital evidence vis-a-vis protection of witnesses/complainants who would otherwise be petrified of reprisal. Digital interventions of BNSS have created far-reaching effects over the anticorruption scenario in India. This could be interpreted as swelling of procedural integrity concomitant with digitalization through BNSS, unto where technology-based investigations, as well as judicial procedures, are sheltered from the slow delays that usually stump anticorruption in India; that digital evidence is seen as solid and undebatable given that it cannot be altered or verified in contradiction as

---

[7] Trung Chinh Dang, Huong Vu Van, et.al., "E-Government and Corruption in an Emerging Country: New Perspectives from a Spatiotemporal Approach", 100 *IREF* 284 (2025).

[8] Isabelle Adam, Mihály Fazekas, "Are Emerging Technologies Helping Win the Fight Against Corruption? A Review of the State of Evidence", available at: https://www.govtransparency.eu/wp-content/uploads/2019/02/ICT-Corruption_GTI-WP-version_2020423.pdf (Visited on April 5, 2025).

an original testimonial. Hence, the reform stands as an unequivocal push for a world where digital vigilance makes ordering of corruption cases swift, transparent, and fair, thus restoring public faith in the rule of law.[9]

India puts the greatest value on interpretations of the courts as to concepts of admissibility and reliability of electronic evidence, more so in anti-corruption trials where a lot of incriminating evidence is maintained in electronic form. The courts have settled a set of principles by a number of landmark decisions that have gone into clarifying how an electronic record must be collected, certified, and produced as evidence. These judgments clarify some of the procedural requirements under Section 65B of the Bharatiya Sakshya Adhiniyam (erstwhile Indian Evidence Act, 1872) - the relevant provision on the question of admissibility of electronic records. In corruption trials where the bulk of primary evidence comprises emails, call recordings, SMS exchanges, bank transaction logs, and video footage, strict compliance with these legal protocols is absolutely critical for fair trial processes and respecting the rights of the accused and the prosecution. By insisting on compliance with these procedural requirements, courts safeguard the sanctity of the judicial process by accepting electronic evidence only where it is reliable and properly authenticated.[10]

This judgment became very significant in anti-corruption cases as investigations are so highly dependent on intercepted communications or recorded conversations, or electronic data of transactions, that any non-compliance with Section 65B could lead to the exclusion of major pieces of evidence. This undue onus was hence cast upon agencies like the CBI and the Enforcement Directorate, wherein these agencies must ensure that proper certification pursuant to Section 65B is obtained during the collection of electronic evidence. At the same time, these grounds might be good enough to lead to a challenge to electronic records by the defense on the argument that they do not comply with Section 65B. Put another way, compliance under Section 65B is not merely that of a procedural hurdle; from a broader perspective, it is the precondition for the admissibility and credibility of an entire case put forward by the prosecution. Thus started this increased annoyed alignment of statutory provisions to prove corruption cases against electronic evidence.[11]

Hence, this ruling finds relevance in the arena of anti-corruption laws. Such investigations almost completely rely on intercepted communications, conversations recorded, or electronic data of transactions from courts; if Section 65B is not complied with, these may be thrown out as the only piece of evidence. Section 65B asks these agencies like the Central Bureau of Investigation and Enforcement Directorate to ensure proper certificate of electronic evidence while collecting such evidence. Meanwhile, this gave a window for opposing counsel to mount defenses against such electronic records that may not be compliant with Section 65B. In other words, the Act is not just a mere procedural hurdle but is, in the real view, the actual prerequisite for the acceptance of the case in evidence and to be worthy of consideration-or treated as true-on the part of the Court. The Anvar P.K. judgment, therefore, raised the bar for proving corruption cases concerning electronic evidence, giving further weight to strict compliance with the statutory provisions therewith.[12]

The Supreme Court in the "*Jagdeo Singh v. the State and Ors.*"[13] decision upheld the stringent test for electronic evidence to be considered in courts. The Court, with stern words, has declared that secondary electronic evidence, such as copies of call data, contents of pen drives on CDs, or photocopies of screenshots, cannot be admitted without a certificate under Section 65B of the Indian Evidence Act, 1872. Any evidence admitted without a certificate has been held illegal, and it cannot be received as evidence of any fact in dispute.

Role of Technology and E-Governance in Anti-Corruption

With the dawn of the technological era, there has been a paradigm shift in the mechanisms employed to combat corruption in India. Technological interventions have done away with certain impurities in corruption that arise from human interface in the execution of service delivery and real-time monitoring. Nowadays, services are rendered wittingly standby for keeping a digital record of all financial transactions and other non-vintage electronic records. All these reduce greatly the scope for manipulation, bribery, and favoritism which operatives in the zenith of corruption in barely few areas of the administration. On the other hand, e-governance has enabled the enhancement of the availability of services and information to citizens, thus reducing their dependence on intermediaries and middlemen, who often facilitated corrupt transactions. Such online programmes resonate, in spirit, with the vision of India under the umbrella of "Digital India" and foster an administrative set-up where transparency, accountability, and integrity become the working ethos of government institutions.

E-governance Initiatives Reducing Corruption

Technology and e-governance thus become tools of transforming paradigms in India's war against corruption. The very nature of technology-based interventions removes major blue prince causes of corrupt practices: human discretion, delayed service delivery, and real-time activity monitoring. Digitally tracked payment mechanisms and digitally recorded, tamper-proof transactions have almost curtailed every instance of manipulation, bribery, favoritism creeping into administrative procedures. An e-governance system has provided increased empowerment to the citizenry toward accessing public services and information, reducing their dependence on intermediaries and middlemen who have predominantly facilitated corrupt transactions. Thus, these digital initiatives consider realizing the vision of India through the "Digital India" campaign for an administrative system where transparency, accountability, and integrity are virtues embedded right into the functioning of the government.[14]

---

[9] Ravindra Kumar, Kaushal Ghunawat, et.al., "Impact of Corruption on Governance and Economic Development: Causes, Consequences, and Solutions", 6 *IJRPR* 702 (2025).

[10] Jamshed Mistry, Abu Jalal, "An Empirical Analysis of the Relationship between E-Government and Corruption", 12 *IJDAR* 163 (2012).

[11] New Perspectives in E-Government and the Prevention of Corruption, available at: https://baselgovernance.org/sites/default/files/2019-06/WP_23_web.pdf (Visited on March 27, 2025).

[12] Manoj Kumar, Abhay Vikram Singh, et.al., "Reshaping Governance Ethics in India: The Need for Reform", 34 *CSS* 174 (2025).

[13] Criminal Appeal no. 527 of 2014.

[14] Suman Goel, Raj Kumar, "E-Governance: A Tool for Tackling the Corruption in India", available at: https://www.researchgate.net/publication/316351067_E-Governance_A_Tool_for_Tackling_the_Corruption_in_India (Visited on February 22, 2025).

Technology merges with e-government in relation to the merger of technology, causing a paradigm shift in corruption in India. A technology-based implementation would exclude all of the major causes behind corrupt practices, such as human discretion, untimely delivery of services, and cash-based transaction monitoring. Digitally tracking the payment process and digitally recording transactions in a tamper-proof manner have hugely prevented possibilities of administrative manipulation, bribery, or favoritism. In principle, e-governance has thus ensured better empowerment of the citizenry in access to public services and information, thereby reducing the middlemen and intermediaries whose assistance is mainly sought in corrupt transactions. Hence, these digital interventions will help India fulfill the vision of creating an administrative system under the "Digital India" campaign where transparency, accountability, and integrity are inherent virtues directly infused in the functioning of the government.

Direct Benefit Transfer (DBT)

The DBT system is one of India's anti-corruption interventions ideally suited for implementation through computer technology to ensure smooth functioning of subsidy and welfare payments. Linking a beneficiary who purportedly has bank accounts to his or her properly authenticated Aadhaar number, the DBT enables payments from government to flow directly into the bank accounts of beneficiaries, thereby avoiding leakages that occur through the hands of intermediaries. The law named "Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016" provides for the Aadhaar biometric verification designed to weed out illegal duplication and forgery in beneficiary transactions. The biggest success of DBT is said to have been in the delivery of LPG subsidy under PAHAL, and it is said that leaks have been cut down by more than ₹50,000 crores per annum-leakages from the OECD Development in Europe provide the numbers in this regard. So, this is a saving for the government account and a big blow to corrupt networks which prospered richly through misappropriations of subsidy funds. Also, DBT with automated transfers had put some degree of predictability and fairness into the welfare distribution system in place of delay and irregularity which corrupt persons perpetrated over time.[15]

E-tendering and E-Procurement

Government contracting and procurement had been the classic areas for corruption, favoritism, and cartelization. E-tendering and e-procurement facilities had been able to provide unprecedented transparency to these processes. CPPP and GeM are some of the major platforms sale course ushering a revolution in these processes. Through these systems, there are provisions for online publication of all tenders notices along with the eligibility criteria and the final evaluation results on a publicly accessible domain. This such a process allows open competition with less discretion left for officials to abuse their powers to favor bidders. It thus enables the tender documents to be viewed in real time and evaluated automatically by the e-tendering system, thus removing any subjectivity in the evaluation and guaranteeing that the evaluation is made by the criteria set long before the tender was floated. This kind of widespread transparency has witnessed a much greater number of bidders, better price discovery, and lower procurement costs, according to MyGov.in. From the perspective of preventing corruption, e-procurement completely eliminates bribery possibilities coupled with placing end-to-end digital records that can be audited and examined should any allegations of impropriety arise, in this manner ensuring constant vigilance over public procurement.

Government E-Marketplace (Gem)

Initiated by the Ministry of Commerce and Industry, Government e-Marketplace has brought a seismic change in the procurement world. Being a fully digital and cashless system, the platform guarantees transparency and efficiency in the process of government purchases. Since its inception in 2016, GeM has transacted over INR Four Lakh crore, which is an indication of how far and wide the initiative has reached. There are no middlemen on GeM; government departments deal directly with the registered sellers and buy goods and services at fair competitive prices. The very processes that GeM has digitized: vendor registration, ebidding, reverse auction, tracking of orders, have eliminated the subjective human intervention which creates a risk of corrupt arrangements between public officials and suppliers. The transparency provided by the digital records acts as a strong deterrent against any alteration in terms after contract awards; hence contracts with the Government are executed according to the verified contract terms. Anti-corruption agencies are empowered to analyze procurement patterns for irregularities using these GeM procurement records and pursue investigations into suspected cases of bid rigging or cartels, hence strengthening the very power to enforce laws.[16]

Bhoomi Project

The experience of the Karnataka Bhoomi Project demonstrates that technology in fact challenges corruption in land administration- a field that is traditionally rife with bribery, manipulation of records, and unwarranted encroachments. This project seeks to digitize over 20 million land records, thereby making land ownership data, mutation records, and transaction history available over the internet for public scrutiny. It, therefore, denies the opportunity to a citizen of corruptly bribing the revenue officials of the particular taluka who had hitherto exercised considerable discretion in land record maintenance. Verified digital records of landholdings facilitate smoother sale transfers and reduce the common incidents of transfer frauds-a sales may be forged in a registration and shall transfer illegal. According to The Guardian, that project has curtailed bribery to a great extent in land deals and thereby, to an extent, safeguard property rights and mitigate disputes in ownership. Further, this digital database helps investigations into corruption cases in land scam and illegal land grants by presenting unimpeachable evidence that can be relied upon to prosecute corrupt practices in this sector.

---

[15] B.K. Mahakul, "E-Governance and Good Governance: The Indian Perceptive", 2 *IJASS* 59 (2014).

[16] T. Alam, M. Aftab, et.al., "Impact of E-Government Initiatives to Combat Corruption Mediating by Behavioral Intention: A Quantitative Analysis from Emerging Economies", 15 *Sustainability* 188 (2023).

Use of Technology in Enforcement

Technopathy is a governing principle for those expert with the art against corruption-working with corruption attempts. Landing high-level investigations faced tremendous challenges vis-a-vis the huge complexities, with increasingly rapidly changing and big corrupt transactions-as if financial crimes are growing to become more sophisticated, scattered over several jurisdictions. Technology provided enforcement agencies some technically advanced tools with which they analyze data, trace financial flows, mixing anomalies in one way or another buried behind thick layers of information. Now, beyond providing and enhancing the investigative capabilities of enforcement agencies to limit human error and to soundly prepare cases backed by credible evidence based on scientific opinion, CBI, ED, and vigilance departments in ministries have also embraced technology to a much greater extent. These technological implements also strengthen enforcement aspects of both control and punishment and make prosecution in corruption-worthy matters proceed faster and more accurately.[17]

AI and Machine Learning for Fraud Detection

With AI tools, any type of research can be conducted, such as sudden spikes in account activity, peculiar contract awards, or collusive behaviors among vendors through bid patterns. AI also analyses their declarations, financial disclosures, and public records in case public servants accumulate assets beyond their means to find inconsistencies suggestive of corruption. This allows enforcement authorities to put their resources in highest-risk areas, thereby streamlining their investigations and mounting more effective cases with solid data backing them. Uncovering hidden corruption networks in massive datasets was a true game changer for the Indian anti-corruption agencies as they chart past enforcement while dealing with complex financial crimes.

Blockchain for Transparent Transactions

Even the blockchain technology, if employed well, may impart transformational changes on transparency and corruption in e-procurement of the government and land administration systems. Its main feature, that of immutability, ensures that once a transaction is recorded on the blockchain, one cannot alter or destroy it without leaving a permanent visible trace. This makes for perfect anti-corruption alternatives in industries rife with graft wherein document forgery, fraudulent registration, or alteration after-the-fact serves as tools for corruption. For example, if integrated with land record management, then land ownership records would be public, all transactions relating to ownership, transfers, and encumbrance of properties would be recorded before the eyes of the public and cryptographically linked one to another in such a way that one transaction to the prior transaction.[18]

Data Analytics for Pattern Recognition

With data analytics being the most proactive tool available for detecting corruption and monitoring public servant activities, agencies responsible for enforcement and oversight have in their armory exceedingly powerful analytics tools that extract meaningful insights from large pools of structured and unstructured data-a feat that is impossible to do manually. An analyst, using different databases for tax records, bank statements, procurement data, travel histories, social media activities, etc., could essentially build thick profiles for public servants-a pattern apparently inconsistent with illicit enrichment or abuse of office could hence warrant probing.

Data analytics has become a critical tool for the proactive detection of corruption and the monitoring of public servants. Enforcement agencies and vigilance departments use these analytics tools to sift through huge pools of structured and unstructured data to draw meaningful insights, which were almost impossible for a manual way. An analyst analyzes data across scattered databases of tax records, bank statements, procurement data, travel histories, social media activities, etc., in essence creating thick profiles on public servants. Any suspicious pattern that raises the thought of illicit enrichment or abuse of office could then be further investigated.

Thus, data analytics is at the very core of purposes of corruption detection and an infringement of corrupt activities by the public servants. The intervention agencies along with the vigilance departments put to use well-crafted analytical software to process tons of structured and unstructured data, drawing inferences that hardly can be drawn in a manual fashion. While the investigators of crime process data tucked inside myriad data repositories such as that of tax records, bank statements, procurement data, travel data, and social media activities, they almost get to profile the public servant and detect suspicious patterns that may suggest illicit enrichment or abuse of office.

Digital Platforms for Whistleblowing and Citizen Reporting

Vigilance departments, for instance, study procurement data to see if certain vendors are consistently showered with contract awards or if there stands some basis for pricing or invoicing patterns that border on being collusive. Travel and financial data could display scenarios where, in the case of being declared or otherwise, a public servant has been found repeatedly going for foreign vacations or acquiring assets. These patterns signal a green light for agencies to launch investigations into areas of immediate concern with evidence, thus strengthening the prosecution's argument in court. By providing a predictive outlook, data analytics aid in the process of risk assessment and may even suggest having an early intervention to contain corruption from

[17] S.K. Reji, B. Moulya, et.al., "E-Governance Evolution: India's Digital Leap from Files to Cloud", 1 *JITTC* 147 (2025).

[18] D.A. Seiam, D. Salman, "Examining the Global Influence of E-Governance on Corruption: A Panel Data Analysis", 10 *FBJ* 216 (2024).

scaling to a higher level. With continuous improvements in the analytical models, anti-corruption agencies throughout India are ultimately designing an intelligent, responsive, and efficient justice system, capable of combating corruption that lies really deep and that is slowly evolving into new forms.[19]

I Paid a Bribe' Platform

The 'I Paid a Bribe' platform represents the use of crowdsourcing to report and document corrupt practices against ordinary people. Established as an NGO initiative, the platform enabled citizens to report instances of bribery wherein they were asked to pay a bribe to avail themselves of some public service anonymously. Funded by the UN Office on Drugs and Crime (UNODC), this platform has fashioned a substantial database: it directs the frequency of occurrence of corruption, the locations where it usually occurs, and the departments one should beware of. I Paid a Bribe eases the means of reporting in contrast to the formal complaint mechanism that requires documentation for legal action: it lets people raise their voices and express their stories without any threat.

As an illustration, the 'I Paid a Bribe' platform documents the successful use of crowdsourcing in exposing, reporting, and recording corrupt practices. This initiative in the digital domain is non-governmental. Citizens can go there anonymously to report incidents when they had to pay bribes to get some public service. Supported by the UN Office on Drugs and Crime (UNODC), the platform has extensively built a data repository that reveals the scale, location, and sectors most vulnerable to corruption. Formal complaints require legal documentation, but 'I Paid a Bribe' is easier for people to share their experience in a protective environment with no threat.

The impact of this platform transcends individual reporting by having aggregated data serve as a major diagnostic tool for policymakers to identify systemic faults, oversee the performance of government departments, and initiate corrective reforms. For instance, if had been the scenario that a lot of reports had been issued against a particular government office or an entire area, then the authorities may consider opening investigations into those serious complaints or take administrative action to correct the matters. Transparency at this level generates so much public attention that no stakeholder may choose to see government institutions shaking and cringing due to allegations of unethical conduct and poor service delivery. With time, such platforms as 'I Paid a Bribe' change the social fabric to reinstate that corruption is no longer simply a private inconvenience but has become a public concern worthy of collective accountability.[20]

Vigilance Clearance Systems

One more aspect of online vigilance in combating corruption is the online vigilance clearance systems. Earlier, the actual clearance of vigilance used to entail endless red tape and formalities. The machinery of unlawful discretion and bribery could have been in full swing through promotions, foreign visits, or contractual approvals. The conversion of these clearance systems, on the other hand, smoothens administrative workings by enforcing transparency and accountability and increasing resistance to manipulation. These systems maintain the clearance requests within the departments in electronic form, may foster an automated deadline for the processing of such applications and in-process real-time updates to the applicants.

In online vigilance clearance systems, acceptance of kharcha-pani has been lowered on account of restricting human discretion and high inter-action between offices and officials and applicants. Transparency is ensured by design, through which decisions are made on the basis of an objective eligibility criterion, which leaves no room for any subjective consideration. Moreover, since these systems maintain an electronic audit trail, oversight agencies can use this trail to scrutinize suspicious decision-making patterns that could flag potential irregularities worthy of consideration for unlawful action. These platforms, as and when implemented within India's administrative setup, help create an environment in which procedure is always respected with integrity. Thus, the vigilance clearance system helps accelerate administration, ensuring that people are convinced of the fairness and just treatment meted out by the government. Thus, in a manner, technology works as a catalyst for change and enhances corruption at various levels of governance.[21]

Conclusion

Any comprehensive treatment of how the country blends technology and e-governance methodologies into its anti-corruption apparatus would conclude that the latter has undergone multidimensional transformation in administrative processes and the processes of enforcing laws. Thus, new culmination points in the realms of technologies include AI, machine learning, blockchain, and data analytics in the detection, investigation, and prevention of corruption. Series of legal reforms have given strong backing to technology usage in fighting corruption and include the Prevention of Corruption Act, 1988; the Information Technology Act, 2000; and the newly created procedural laws under the Bharatiya Nagarik Suraksha Sanhita, 2023. Coupled with judicial pronouncements on the admissibility of suitably authenticated electronic evidence, all these ensure that modern-day corruption cases can be disposed of with pinpoint accuracy, integrity, and fairness. An amalgamation of these advances in technology and law thus modernized India's enforcement capacity while furthering the country's commitment toward transparency and accountability at all levels of governance.

Suggestions

1. Expand Blockchain-Based Pilot Projects in Land Records and Procurement to Additional States, Ensuring Real-Time Transparency and

[19] Fighting Corruption with E-Government Applications, available at: https://www.unapcict.org/sites/default/files/2019-01/enote8.pdf (Visited on March 15, 2025).

[20] ICT as a Tool for Citizen Participation in Anti-Corruption Efforts, available at: https://www.unodc.org/e4j/ru/anti-corruption/module-10/key-issues/ict-as-a-tool-for-citizen-participation-in-anti-corruption-efforts.html (Visited on April 2, 2025).

[21] Sangit Sarita Dwivedi, "Enabling Good Governance through E-Governance in India: Moments for Retrospection", available at: https://www.internationalconference.in/XVI_AIC/TS1_pdf/3.%20Sangit%20Sarita%20Dwivedi.pdf (Visited on March 10, 2025).

Tamper-Proof Documentation Across High-Risk SectOrs

2. Mandate Regular AI-Driven Audits in Government Financial Systems to Proactively Identify Anomalies in Fund Disbursement, Procurement, and Contract Management.
3. Upgrade Training for Law Enforcement on the Technical Handling and Certification of Electronic Evidence under Section 65B to Prevent Evidentiary Lapses During Prosecution.
4. Integrate Public Feedback Mechanisms Directly Into Digital Platforms Like Gem and DBT Portals, Allowing Users to Report Inefficiencies or Suspected Misconduct Anonymously.
5. Develop Centralized Data-Sharing Protocols Among Enforcement Agencies, Ensuring Seamless Access to Financial, Property, and Identity Records for Comprehensive Investigations.
6. Enact Periodic Independent Audits of Digital Anti-Corruption Platforms to Verify Data Integrity, System Security, and Institutional Compliance with Transparency Standards.
7. Introduce Legislative Amendments Mandating Audiovisual Recording of All High-Value Procurement Negotiations, Adding a Layer of Verifiable Accountability.
8. Launch Public Education Campaigns Explaining Citizen Rights under RTI and Digital Whistleblower Protections, Encouraging Wider Participation in Reporting Corruption.
9. Establish a Secure, Government-Backed National Whistleblower Portal Integrating Existing Platforms Like ‘i Paid a Bribe’ with Legal Protections and Investigation Triggers.
10. Create AI-Powered Risk Scoring Models for Public Servants, Flagging Unusual Wealth Accumulation or Lifestyle Indicators for Preventive Internal Vigilance Reviews.