# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

# DISCLAIMER

 ISSN: 2582-6433

# EDITORIAL TEAM

## EDITORS

### Dr. Samrat Datta

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*

### *Dr. Namita Jain*

*Head & Associate Professor*

*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*

*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*

 ISSN: 2582-6433

# Mrs.S.Kalpana

Assistant professor of Law

*Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*

# Avinash Kumar

*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

 ISSN: 2582-6433

# ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

# THE TRANSFORMATIVE INFLUENCE OF POST-COVID TECHNOLOGIES ON CRIMINAL INVESTIGATIONS AND PROSECUTIONS IN THE INDIAN CRIMINAL JUSTICE SYSTEM

AUTHORED BY - JISHA JASMIN A*[1]

## Abstract

The aftermath of the COVID-19 pandemic has underlined the significance of technology in reforming various sectors of society including the criminal justice system of India. In India where the legal background was already undergoing changes because law change according to the society's change. The Indian criminal justice system has been significantly impacted by advancements in technology over the past few decades. New technologies have revolutionized the way criminal investigations are conducted and prosecutions are pursued. The pandemic acted as a catalyst in appositive sense, and it is accelerating the adoption of new technologies in criminal investigations and prosecutions in our Criminal Justice System. This article explores the profound impact of post-COVID technologies on the Indian Criminal Justice System, shedding light on both opportunities and challenges. And explores the multifaceted impact of new technologies on the Indian criminal justice system, including their role in evidence collection, forensic analysis, and surveillance and the challenges and concerns they raise. Looking to the Technological Innovations in Criminal Investigations we can see that in the wake of the pandemic, the limitations imposed on physical interactions necessitated the utilization of technology to sustain crucial criminal investigations. For example, in the case of advanced data analytics, machine learning algorithms and artificial intelligence have played pivotal roles in processing vast amounts of data for identifying the patterns and predicting potential criminal behaviour. So, these technologies aid law enforcement agencies in detecting and preventing crimes, particularly cybercrimes, which saw a surge during the pandemic due to increased online activities

*Research Scholar, Government Law College, Trivandrum, University Of Kerala.

 ISSN: 2582-6433

## Introduction

The Post-COVID era has ushered in a new era of technological advancement in the Indian Criminal Justice System. While these technologies offer unprecedented opportunities for efficient investigations and prosecutions. Even though it also come with ethical dilemmas and challenges that require careful navigation. Striking a balance between harnessing the potential of technology and safeguarding individual rights is crucial to building a resilient and equitable criminal justice system for the digital age. By embracing these changes and addressing associated challenges, India can pave the way for a more efficient, accessible, and just legal system.

As we know that the emergence of the COVID-19 pandemic in 2019 brought about an unprecedented need for technological solutions across various sectors, including the criminal justice system. As physical interactions became limited, the Indian criminal justice system underwent a rapid transformation in its investigative and prosecutorial processes. The closure of physical spaces including Police stations and Courts had led to the rapid adoption of virtual collaborative tools. These tools enabled investigators, lawyers, and other stakeholders to collaborate seamlessly and regardless of their geographical locations. Virtual hearings and remote Court proceedings became the norm, and it is ensuring that the wheels of justice continued to turn even during lockdowns. This transformation while driven by necessity has ushered in a more accessible and efficient justice system. The digital era has brought about an array of tools for evidence gathering including digital forensics, biometric technologies, and facial recognition systems. These tools not only expedite the identification of suspects but also aid in reconstructing crime scenes and corroborating evidence. Furthermore, the increased use of surveillance technologies has led to the capture of real-time evidence and thereby enhancing the efficacy of criminal investigations.

While the integration of technology has yielded numerous benefits, and it has also given rise to significant challenges and ethical dilemmas. Privacy concerns have intensified because as increased data collection and surveillance could infringe upon individual rights. Moreover, the potential for biases in algorithms used in predictive policing and facial recognition systems has raised questions about the fairness and objectivity of criminal investigations. The proliferation of technology has opened new avenues for cybercriminals to exploit vulnerabilities. As criminal investigations increasingly involve digital evidence, ensuring the security and integrity of data becomes paramount. Strengthening cyber security measures and enacting robust data protection regulations are imperative to safeguard both investigative processes and individual privacy. The

 ISSN: 2582-6433

adoption of new technologies necessitates corresponding legal reforms to accommodate their impact on criminal investigations and prosecutions. The Indian legal framework must be flexible enough to address the evolving challenges while upholding the principles of justice and fairness. Legislation concerning cybercrime, digital evidence, and data protection needs to be continually updated to reflect the changing technological landscape.

The COVID-19 pandemic disrupted traditional norms and practices, forcing governments and institutions worldwide to adopt innovative solutions to maintain essential functions. The Indian criminal justice system faced unique challenges due to its reliance on physical interactions and paper-based processes. To ensure the continuity of justice, the adoption of post-COVID technologies became essential. This article examines the transformative influence of these technologies on criminal investigations and prosecutions in the Indian criminal justice system. By examining virtual evidence collection, forensic advancements, data analytics, virtual court proceedings, e-filing, case management, and block chain technology, this research explores how these innovations have reshaped the landscape of criminal justice processes. The paper also discusses the challenges posed by the digital divide, data privacy, security, and legal and ethical concerns associated with these technological advancements.

## Technological Transformation in Criminal Investigation

*Virtual Evidence Collection*: Traditional methods of evidence collection often required physical presence which causing delays during lockdowns. The limitations imposed by lockdowns and social distancing necessitated a shift towards virtual evidence collection techniques. The post-COVID era introduced virtual evidence collection techniques including remote interviews, video conferencing and virtual crime scene reconstructions. This has expedited investigations while adhering to health and safety guidelines. The advent of virtual courtrooms and online platforms has introduced a significant degree of flexibility and accessibility to legal proceedings. This is especially crucial in times of crises in the COVID-19 pandemic, when in-person appearances became challenging. Virtual hearings have reduced the backlog of cases and expedited the legal process, making justice more accessible to a wider range of individuals[2].

*Forensic Advancements*: The integration of advanced forensic technologies such as DNA analysis, facial recognition and digital forensics has revolutionized evidence collection and analysis. These

[2]https://vakilsearch.com/blog/the-transformative-impact-of-new-technologies-on-criminal-law-andinvestigations (last visited on October 10, 2023).

 ISSN: 2582-6433

technologies enhance accuracy in suspect identification and provide irrefutable evidence in Court. Forensic science has seen tremendous advancements, largely thanks to technology. DNA analysis, for instance, has revolutionized criminal investigations. The accuracy of DNA profiling has exonerated innocent individuals and identified perpetrators in cases that were once unsolvable. Additionally, advancements in fingerprint and ballistics analysis have made it possible to connect physical evidence to suspects with a higher degree of certainty[3].

*Data Analytics*: The exponential growth of digital data has led to the adoption of data analytics tools in criminal investigations. These tools help law enforcement agencies identify patterns, predict criminal activities and present evidence-backed cases for prosecution. The explosion of digital data has necessitated the use of data analytics tools to mine information, identify patterns, and establish connections. This aids law enforcement agencies in predicting and preventing criminal activities while providing valuable insights for effective prosecutions. The power of big data and analytics cannot be underestimated in the realm of law enforcement. Police departments can now harness vast amounts of historical crime data to predict where and when crimes are likely to occur. This proactive approach allows for more strategic resource allocation, ultimately leading to crime prevention and safer communities[4].

*Digital Evidence and Forensics*: Post-COVID technologies catalysed the shift towards digital evidence collection and analysis. Law enforcement agencies increasingly rely on data retrieved from electronic devices, social media, and online platforms. This transition enables a more efficient collation and presentation of evidence, expediting investigations and reducing the reliance on traditional methods.

*Artificial Intelligence and Predictive Policing*: The integration of artificial intelligence (AI) in criminal investigations has revolutionized the identification of patterns and trends. Predictive policing algorithms analyse historical data to forecast potential crime hotspots, aiding law enforcement in proactive measures. However, concerns over bias and discriminatory outcomes must be addressed to ensure the ethical use of AI.

*Remote Interrogations and Virtual Reality Reconstructions*: Social distancing norms led to the adoption of remote interrogation methods, where suspects, witnesses, and experts could provide

[3] Ibid
[4] ibid

 ISSN: 2582-6433

statements virtually. Additionally, virtual reality reconstructions of crime scenes facilitate a comprehensive understanding for investigators and judges alike. These tools minimize physical presence requirements while maximizing the accuracy of information.

*Enhanced Evidence Gathering*: Technology has fundamentally transformed the way evidence is gathered. In the digital age, smartphones have become ubiquitous, and nearly everyone carries a portable, high-quality camera in their pocket. This has made it easier to capture critical evidence, such as photos, videos, and audio recordings, often in real time. These digital records are difficult to dispute, providing a more accurate representation of events, thereby strengthening cases. Moreover, advancements in surveillance technology, including facial recognition systems and license plate recognition cameras, have bolstered the capabilities of law enforcement agencies. These tools are instrumental in identifying suspects and tracking criminal activity.

*Streamlined Case Management*: The digital era has ushered in a plethora of software solutions designed to streamline case management for legal professionals. These tools enable lawyers and investigators to efficiently organize and access vast amounts of information. From legal research databases to case management software, technology has significantly reduced the time spent on administrative tasks and allowed legal experts to focus on the core aspects of their cases.

## Technological Advancements in Prosecutions

*Virtual Court Proceedings*: Virtual Court proceedings emerged as a solution to the backlog of cases during the pandemic. These proceedings expedite trials, improve access to justice, and reduce costs for all parties involved. The pandemic catalyzed the shift towards virtual Court proceedings. This innovation significantly reduces the backlog of cases, expediting trials and ensuring access to justice. Virtual hearings also lower costs for litigants and lawyers. To mitigate the backlog of cases, virtual court proceedings became a viable alternative. Video conferencing platforms allowed judges, lawyers, and witnesses to participate remotely, enhancing accessibility to justice. However, ensuring due process and preventing technical glitches are on-going challenges.

*E-Filing and Case Management*: The transition to electronic filing systems and digital case management tools has streamlined administrative processes. This shift improves transparency, reduces paperwork, and facilitates seamless sharing of documents among stakeholders. The adoption of electronic filing systems and digital case management tools has streamlined

 ISSN: 2582-6433

administrative processes. This ensures transparency, reduces paperwork, and simplifies the sharing of documents between parties involved in criminal cases. The digital transition extended to case management, with the adoption of e-filing systems that facilitate the submission and tracking of legal documents. This expedites case progression, minimizes paperwork, and improves transparency.

*Blockchain for Transparency*: The Indian criminal justice system has grappled with issues of corruption and lack of transparency. Blockchain technology can secure evidence, maintain custody chains, and create tamper-proof records, ensuring the integrity of the legal process. Blockchain technology offers a solution to issues of corruption and transparency in the Indian criminal justice system. By securing evidence and maintaining tamper-proof records, blockchain ensures the integrity of legal proceedings.

*Sentencing and Correctional Technologies*: Technological advancements also influence post-conviction stages. Sentencing algorithms consider various factors to recommend appropriate sentences, striving for consistency and fairness. Additionally, electronic monitoring and rehabilitation programs provide innovative alternatives to traditional incarceration.

## Advancements in Evidence Collection

*Digital Evidence*: The rise of smartphones and social media platforms has led to an increase in the availability of digital evidence in criminal cases. Digital evidence includes text messages, emails, videos, and photographs, which are crucial in establishing guilt or innocence. The Indian Evidence Act, 1872, was amended in 2000 to accommodate digital evidence, providing a legal framework for its admissibility[5].

*DNA Profiling*: DNA profiling has become a powerful tool in criminal investigations and prosecutions. The establishment of DNA laboratories across India has facilitated the use of DNA evidence in solving crimes and establishing paternity[6].several landmark cases related to DNA profiling in India have shaped the legal landscape. The most notable is the Selvi vs. State of Karnataka[7] case in 2010, where the Supreme Court addressed the admissibility of narcoanalysis, brain mapping and polygraph testing. Some of the notable cases in India have involved DNA

[5]Indian Evidence Act, 1872, s. 65B
[6]Natarajan, J. (2012). DNA Profiling in India: The Current Scenario. Journal of Indian Academy of Forensic Medicine, 34(3), 263-267
[7] 2010(7) SCC 263

 ISSN: 2582-6433

profiling:

1. Aarushi-Hemraj Murder Case (2008)[8]: The DNA analysis was a significant aspect of the investigation into the murders of Aarushi Talwar and Hemraj Banjade.
2. Mumbai Terror Attacks (2008)[9]: DNA testing was utilized to identify the terrorists involved in the Mumbai attacks.
3. Gudiya Rape Case (2017)[10]: DNA evidence played a key role in identifying and convicting the perpetrator in the brutal rape and murder of an eight-year-old girl in Jammu and Kashmir.
4. Kathua Rape Case (2018)[11]: DNA profiling was used to establish the identity of the victim and the accused in the heinous rape and murder of an eight-year-old girl in Jammu and Kashmir.
5. Nithari Serial Killings (2006)[12]: In this case the DNA evidence played a crucial role in convicting Surinder Koli for the murders of several children in Nithari.

These cases highlight the increasing importance of DNA profiling in criminal investigations and justice delivery in India.

*Forensic Analysis*: Cyber forensics plays a pivotal role in investigating cybercrimes, including hacking, online fraud, and cyber bullying[13].The Central Bureau of Investigation (CBI) and State police departments have established specialized cybercrime units to handle such cases. Notable cases involve the use of forensic analysis include the Aarushi Talwar murder case, the Nirbhaya gangrape case and the Mumbai attacks. Each cases involves different forensic technique to gather evidence and establish facts in court.

*Automated Fingerprint Identification Systems (AFIS)*: AFIS technology has sped up identifying and matching fingerprints in criminal cases[14].It has been used to solve cold cases and link suspects to multiple crimes.

*Surveillance Technologies*: It mainly includes Closed-Circuit Television (CCTV) Cameras and

[8] *Mohammed Ajmal Mohammed Amir Kasab @ Abu Mujahid v. State of Maharashtra* (2012)8 S.C.R 295
[9] *Zahur Haidar Zaidi v. C B I*, SLP (Crl.) No.2123 of 2018
[10] *Mohd. Akhtar v. State of Jammu and Kashmir*, SC WP(Crl.) No. 85 of 2018
[11] *Surendra Koli v. State Thru C.B.I*, 2023:AHC: 199091-DB
[12] *Dr. (Smt.) Nupur Talwar v. Sate of U. P And Anr* (1984) 2 SCC 627
[13] Central Bureau of Investigation (CBI). (n.d.). Cyber Crime
[14] National Crime Records Bureau (NCRB). (2020). Automated Fingerprint Identification System (AFIS).

 ISSN: 2582-6433

Phone Tapping and Interception. In the widespread installation of CCTV cameras has enhanced surveillance capabilities in public spaces, aiding in the prevention and investigation of crimes[15].However, concerns about privacy and misuse of surveillance data have arisen. Law enforcement agencies can legally intercept phone conversations under the provisions of the Indian Telegraph Act, 1885, and the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009[16].Striking a balance between national security and individual privacy remains a challenge. Several cases in India have addressed the use and regulation of surveillance technology. For example, the Justice KS Puttaswamy (Retd.) and Anr. v. Union of India Case[17] in 2017 recognized the right to privacy as a fundamental right. Additionally, the Puttaswamy judgment led to discussion about the need for a robust data protection framework.

## Disadvantages of using Technology in Criminal Investigations and Prosecution

The integration of technology into criminal investigations and prosecution has revolutionized the criminal justice system, enhancing its efficiency and accuracy. However, while technological advancements have undoubtedly brought numerous advantages, it is crucial to acknowledge the potential disadvantages that arise from overreliance on technology. The downsides of using technology in criminal investigations and prosecution, with real-world examples to illustrate these issues.

*Privacy Concerns*: One of the most significant disadvantages of using technology in criminal investigations is the potential infringement on privacy rights. The collection and utilization of vast amounts of personal data, such as phone records, emails, and social media profiles, can raise serious privacy concerns. For instance, in the case of United States v. Jones[18], law enforcement used a GPS tracking device to monitor a suspect's vehicle without a warrant, leading to a Supreme Court ruling that such surveillance violated the Fourth Amendment. The increased reliance on technology for surveillance and data collection has raised valid concerns about individual privacy. It’s essential to strike a balance between public safety and personal privacy rights. The proliferation of surveillance cameras and data tracking tools means that people are often under

[15] Ministry of Home Affairs, Government of India. (2021). Guidelines for CCTV Surveillance in India
[16] Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009
[17] (2017) 10 SCC 1
[18] 565 U S 400 (2012)

 ISSN: 2582-6433

constant observation, and this can lead to a sense of surveillance creep and violations of privacy.

*Bias and Discrimination*: Technological tools like predictive policing algorithms and facial recognition software can perpetuate and exacerbate existing biases in the criminal justice system. For instance, a study by the American Civil Liberties Union (ACLU) revealed that facial recognition software had a significantly higher error rate when identifying individuals with darker skin tones, leading to potential misidentifications and wrongful arrests.

*Data Integrity and Security*: The reliability of evidence collected through technology can be compromised due to data tampering or cyberattacks. In 2019, the Baltimore Police Department experienced a ransomware attack that disrupted their ability to access critical case-related data, raising concerns about the security of electronic evidence in criminal cases.

*Overreliance on Technology*: Overreliance on technology may lead to investigators and prosecutors neglecting traditional investigative techniques, such as interviewing witnesses and collecting physical evidence. This overreliance can result in missed opportunities, as was evident in the Boston Marathon bombing case, where surveillance cameras played a crucial role, but traditional investigative methods were not as diligently pursued.

*Resource Allocation*: Investing in advanced technology can be costly, diverting resources from other areas of the criminal justice system, such as community policing or rehabilitation programs. This misallocation of resources may not necessarily lead to a safer society and may perpetuate the cycle of crime by not addressing its root causes.

*Complex Legal Issues*: Technological advancements often outpace the development of legal frameworks and precedents, leading to complex legal issues. For example, the use of drones in law enforcement is still a topic of debate, with concerns regarding the Fourth Amendment rights of individuals in private spaces.

*Expertise Gap*: The effective use of technology in criminal investigations and prosecutions often requires specialized expertise. This can create a gap between agencies with access to such expertise and those that do not. Smaller law enforcement agencies may find it challenging to keep up with the rapid pace of technological advancement.

 ISSN: 2582-6433

*Data Security Risks*: The digitalization of legal processes also introduces significant data security risks. Sensitive information related to ongoing investigations, witness testimonies, and personal data can be vulnerable to hacking and data breaches. Safeguarding this information is paramount, necessitating robust cyber security measures.

*Technological Disparities*: The digital divide is a pressing concern. Not everyone has equal access to technology, which can result in disparities in access to legal services and justice. Those who are digitally disadvantaged may find it more challenging to participate fully in legal proceedings, potentially compromising their rights.

*Human Error and Bias*: While technology can enhance many aspects of criminal law and investigations, there's always the risk of human error in its application. Additionally, algorithms and AI systems used in predictive policing and sentencing can inadvertently perpetuate biases present in historical data. Striking a balance between automation and human oversight is critical to ensure fairness and accuracy.

While technology has brought significant benefits to criminal investigations and prosecutions, it is essential to recognize and address the associated disadvantages. Privacy concerns, bias, data integrity, overreliance, resource allocation, legal complexities, and expertise gaps are real challenges that need to be carefully considered in the pursuit of justice. Striking a balance between leveraging technology and preserving fundamental rights and principles is crucial for a fair and effective criminal justice system. Lawmakers, law enforcement agencies, and legal professionals must work together to mitigate these disadvantages and ensure that technology serves justice without compromising essential values and safeguards.

## Challenges And Considerations

*Legal Framework Adaptation*: One of the primary challenges lies in adapting legal frameworks to keep pace with the rapid evolution of technology. Laws that were formulated before the digital age may not adequately address novel situations created by emerging technologies. For instance, questions surrounding the admissibility of evidence obtained from emerging surveillance technologies like drones or the legal status of cryptocurrencies in cases involving financial crimes require constant updates to existing legislation.

*Cybercrime Complexity*: The digital era has given rise to complex forms of criminal activity, often

 ISSN: 2582-6433

collectively referred to as cybercrime. These include hacking, identity theft, and various types of online fraud. Investigating and prosecuting cybercrimes presents unique challenges, as the perpetrators can be geographically dispersed and may exploit legal jurisdictional gaps.

*Digital Evidence Authentication*: Ensuring the authenticity of digital evidence is a critical challenge. The ease with which digital content can be manipulated, forged, or misrepresented necessitates stringent procedures for its authentication. Legal systems must continually evolve to establish protocols that validate the integrity of digital evidence.

*Ethical Dilemmas*: The application of emerging technologies, particularly artificial intelligence (AI), in criminal justice systems introduces ethical dilemmas. For example, the use of AI algorithms for predictive policing and sentencing decisions raises concerns about bias and fairness. Ensuring that technology is used ethically and that decision-making processes are transparent and accountable is a complex yet vital challenge.

## Suggestions For using Technology

*Continuous Education and Training*: Given the rapid evolution of technology, legal professionals, including judges, lawyers, and law enforcement personnel, should receive ongoing education and training in technology-related matters. This includes staying updated on new technologies, their legal implications, and best practices for their use in criminal cases.

*Robust Cyber security Measures*: Protecting the integrity and confidentiality of digital information is paramount. Implementing and continually updating robust cyber security measures within legal systems, law enforcement agencies, and legal firms can help safeguard sensitive information from cyber threats.

*Ethical AI Use*: Establish clear guidelines and regulations for the ethical use of AI in the criminal justice system. This includes ensuring transparency in AI algorithms used for decision-making, regularly auditing these algorithms for bias, and providing mechanisms for accountability in cases where AI systems are involved in critical decisions, such as sentencing.

*Collaborative Partnerships*: Foster collaborative partnerships between law enforcement agencies, technology companies, legal experts, and civil rights organizations. Collaborative efforts can lead to the development of innovative solutions, the formulation of sound legal frameworks, and the

 ISSN: 2582-6433

identification of potential pitfalls associated with technology in the legal domain.

*Public Awareness and Participation*: Engage the public in discussions about the impact of technology on criminal law and investigations. Encourage citizen participation in shaping policies and regulations to ensure that technological advancements align with societal values and principles of justice.

*Digital / Technological Divide and Accessibility*: While technology offers numerous benefits, its unequal distribution raises accessibility issues. Socioeconomic disparities may prevent certain individuals from fully participating in virtual proceedings or benefiting from advanced investigation methods. Measures to bridge this gap are imperative. Despite technological advancements, the digital divide remains a barrier to equitable access. Many individuals, especially in rural areas, lack the necessary resources to participate in virtual proceedings.

*Data Privacy and Security*: The extensive use of surveillance technologies raises concerns about violations of privacy rights guaranteed under the Indian Constitution[19].The Supreme Court of India has issued guidelines to ensure the lawful and proportionate use of surveillance techniques[20].The increased reliance on digital evidence raises concerns about privacy and data security. Safeguarding sensitive information from unauthorized access and ensuring compliance with data protection laws are paramount. Striking a balance between investigative needs and individual rights is crucial. With the reliance on digital evidence, concerns about data privacy and security have arisen. Stringent measures are required to safeguard sensitive information and prevent unauthorized access.

*Legal and Ethical Concerns*: The adoption of emerging technologies like facial recognition and predictive analytics necessitates addressing legal and ethical concerns related to privacy, bias, and individual rights.

*Legal Admissibility of Technological Evidence*: The admissibility of digital evidence in court poses challenges. Ensuring the integrity and authenticity of evidence, along with addressing concerns of tampering, require robust legislative and procedural frameworks. Courts must be equipped to assess and validate technological evidence effectively.

[19] The Constitution of India, Part III, Art. 21.
[20] *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*, (2017) 10 SCC 1

 ISSN: 2582-6433

*Digital Forensics Capacity*: There is a need to strengthen the capacity of law enforcement agencies in the field of digital forensics to effectively handle the increasing volume of digital evidence[21].Training programs and the establishment of state-of-the-art forensic labs are essential. *Cybersecurity Threats*: As technology advances, so do cyber threats, making it necessary for law enforcement to continuously adapt and upgrade their capabilities[22].Collaboration with the private sector and international agencies is vital to combat cybercrimes effectively.

## Conclusion

New technologies have undeniably transformed criminal investigations and prosecutions in the Indian criminal justice system. They have enhanced evidence collection, forensic analysis, and surveillance capabilities. However, the implementation of these technologies must be accompanied by a robust legal framework to protect individual rights and privacy. Striking a balance between law enforcement needs and civil liberties will be an ongoing challenge as technology continues to evolve. The post-COVID era has catalyzed a technological revolution in the Indian criminal justice system. The integration of advanced tools for investigations and prosecutions has the potential to accelerate the legal process, reduce backlog, and enhance transparency. However, a careful approach is essential to address challenges such as the digital divide, data security, and ethical considerations. As India continues to embrace these transformative technologies, it has an opportunity to shape a more efficient, accessible, and fair criminal justice system for the future. The incorporation of post-COVID technologies into the Indian criminal justice system has brought about significant transformations in investigations and prosecutions. While these innovations hold immense potential to expedite the legal process and improve transparency, challenges such as the digital divide, data security, and ethical considerations must be carefully navigated. The Indian criminal justice system stands at a crossroads, where the intelligent integration of technology can lead to a more efficient, accessible, and equitable future for all stakeholders involved.

The post-COVID era has accelerated the integration of technologies in the Indian criminal justice system, transforming the landscape of investigations and prosecutions. As digital evidence, AI, virtual proceedings, and other innovations become more ingrained, stakeholders must collaborate to navigate challenges and maximize the benefits. The Indian criminal justice system stands at a

[21] Ministry of Electronics and Information Technology, Government of India. (2020). Scheme for Financial Assistance to States for Setting up of Cyber Crime Prevention against Women and Children (CCPWC) Units.
[22] National Cyber Security Policy, Government of India, 2013

 ISSN: 2582-6433

pivotal juncture, where the prudent and ethical use of technology can enhance efficiency and fairness, ultimately upholding the rule of law. Balancing innovation with fundamental rights will be essential to harness the transformative potential of post-COVID technologies. The COVID-19 pandemic reshaped the world in profound ways, forcing societies to adapt to unprecedented challenges. One sector significantly impacted is the criminal justice system, prompting the adoption of innovative technologies to ensure the continuity of investigations and prosecutions. In India, where the criminal justice system has faced numerous challenges, the post-COVID era has witnessed a rapid integration of technology, revolutionizing the landscape of criminal investigations and prosecutions.

## References:


- Central Bureau of Investigation (CBI). (n.d.). Cyber Crime. Retrieved from https://www.cbi.gov.in/quick-links/cyber-crime.
- Indian Evidence Act, 1872, s. 65B.
- Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009.
- Ministry of Electronics and Information Technology, Government of India. (2020). Scheme for Financial Assistance to States for Setting up of Cyber Crime Prevention against Women and Children (CCPWC) Units.
- Ministry of Home Affairs, Government of India. (2021). Guidelines for CCTV Surveillance in India.
- Natarajan, J. (2012). DNA Profiling in India: The Current Scenario. Journal of Indian Academy of Forensic Medicine, 34(3), 263-267.
- National Crime Records Bureau (NCRB). (2020). Automated Fingerprint Identification System (AFIS).
- National Cyber Security Policy, Government of India, 2013.
- The Constitution of India, Part III, Art. 21.
- Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, (2017) 10 SCC 1.
- Mohammed Ajmal Mohammed Amir Kasab @ Abu Mujahid vs State of Maharashtra (2012)8 S.C.R 295
- Zahur Haidar Zaidi vs C B I on 19 January 2018 on 7 May 2018
- Mohd. Akhtar vs State of Jammu and Kashmir
- Surendra Koli vs State Thru C.B.I on16 October 2023.

 ISSN: 2582-6433


- Dr. (Smt.) Nupur Talwar vs Sate of U. P And Anr (1984) 2 SCC 627
- Central Bureau of Investigation (CBI). (n.d.). Cyber Crime
- National Crime Records Bureau (NCRB). (2020). Automated Fingerprint Identification System (AFIS).
- Selvi vs. State of Karnataka 2010(7) SCC 263
- United States v. Jones 565 U S 400 (2012)