MODERNIZING JUSTICE: THE INFLUENCE OF TECHNOLOGY ON CRIMINAL LAW

Baivabi Priyadarshini, [B.A. LL.B. (H), LL.M.], Symbiosis International (Deemed University)

ABSTRACT

Information technology solutions have created new opportunities for internet-based business networking in the era of rapidly developing technologies, including e-banking. These solutions seek to save expenses, make complicated financial transactions easier, and offer quicker, more effective ways. The aim of this research is to offer a comprehensive comprehension of the relationship between criminal law and technology. It attempts to solve the problems brought about by the pervasive use of the internet and its applications in the modern world. We examine how technology and the criminal justice system interact in this study. Our investigation covers the uses, advantages, difficulties, and moral issues related to technological integration. We examine the ways that facial recognition, risk assessment algorithms, and predictive policing are changing criminal justice, law enforcement, and prisons. We also stress the importance of accountability, justice, and openness when implementing technology in the criminal justice system. The growing trend of people depending on technology to handle their workloads makes it imperative to identify workable solutions. Modern banking, reservations for trains, and airline transactions all depend on state-of-the-art technology. The modern generation is largely dependent on technology since computers enable efficient procedures and streamlined operations. While the spread of IT facilities has many benefits, there are drawbacks as well. Among these difficulties, cybercrime stands out as a unique mobile and computer security offense. India's criminal law and technology confluence has experienced significant changes, mainly because of continuous digital transformation and technical breakthroughs.

Keywords: cybercrimes, teenager access crime, digital evidence, IT Act, IPC, offences, criminal justice

INTRODUCTION

Given that the globe is now digitally connected, our dependence on technology has only grown. Modern approaches to digital and cyber technologies have been made possible by the COVID-19 pandemic. One may see how this shift affects how one lives at home and at work, altering one's manner of living. Technology has had a big impact on how society is changing. While it has made many aspects of daily life easier to deal with, it has also given antisocial elements and criminals a platform to exploit its possibilities in various ways, leading to new forms of fraud and intrusion related to credit/debit card forgeries and ATMs. We employ digital forms, computers, and cellular technologies daily. These technologies improve data storage, which enables processing information at very high speeds and low latency, as well as sharing or communicating inside or across enterprises, agencies, states, and nations. This modernization represents a change from the colonial laws of the past to the legal systems of today. The Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023, have been introduced to commemorate this. Long-standing laws like the Indian Penal Code of 1860 and the Code of Criminal Procedure of 1973 would be superseded by these new laws. In this way, India's commitment to a just and fair legal system in the digital age will be further reaffirmed as efficiency, accountability, and accessibility to justice are recapitalized while meeting the needs of the modern society about its issues.[1] The society is being significantly impacted by the constant advancements in technology. For example, when a new technology is introduced into society, people take some time to get used to it and it isn't fully spread. Meanwhile, another novel technology is introduced, which primarily causes chaos when it comes to learning technology for the average person. However, criminal and antisocial elements are quick to upgrade themselves with the newest technology and misuse it for their own gain, which leaves people vulnerable to cybercrime and cyberfraud. This has a significant effect on the present criminal scenario and presents new difficulties for the criminal justice system.

The Indian judicial system has performed the very basic functions of interpreting and declaring laws under criminal law and technology. Such landmark judgments, be it in the case of Puttaswamy (JUSTICE KS PUTTASWAMY (RETD) V. UOI, 2018), reaffirming the right to

[1] Gupta, R. R., & Srivastava, A. (2023). Impact of emerging technology on recent criminal scenario. *IP International Journal of Forensic Medicine and Toxicological Sciences*, *8*(2), 65–68. https://doi.org/10.18231/j.ijfmts.2023.013

privacy, or Shreya Singhal (Shreya Singhal & ors. V. Union of India, 2015), striking down unconstitutional provisions of the IT Act, highlight this. The Indian Computer Emergency Response Team is aided by various law enforcement agencies, Cyber Crime Cells, and Cyber Crime Investigation Cells of central agencies in mitigating cyber threats and enforcement pertaining to compliance with cybersecurity. Recent developments, through new criminal legislations and changes in many existing laws, have kept pace with the dynamic process of digital transformation.

LITERARTURE REVIEW

Digital evidence has become the hallmark of modern criminal investigations and prosecutions. Improvements in technology have gone hand in glove with the proliferation of digital data in forms of emails, social media posts, and electronic transactions, among many others. Researchers indicate that digital evidence can provide very valuable insights into criminal activities and also link suspects with criminal activities (Casey, 2011). However, challenges unique in themselves are presented with the handling and admissibility of that digital evidence; these include problems relating to data integrity and chain of custody (Kerr, 2010).

E-discovery, in other words, refers to "the process of seeking, locating, securing, preserving, and ultimately analyzing electronic data to be used as evidence in court" (Brenner, 2009).Tremendous growth in the volume and complexity of digital data has resulted in e-discovery becoming one of the most crucial yet challenging fronts in criminal litigation. In fact, legal scholars, it is being stated, have strongly felt that there is an urgent call for new guidelines and standards to stop growing outrage over issues of data privacy, relevance, as well as abuse regarding potential utility (., 2015).

Cybercrime is any illegitimate action that makes use of a network or device, including hacking, identity theft, or fraud. Because of the exponential growth of the internet and other forms of digital communication, cybercrime has also increased, thereby requiring some special legal provisions in the law provisions and law enforcement mechanisms (Norton, 2018). Researchers have indicated that conventional criminal law very often fails to resolve the special problems associated with cybercriminals and therefore needs the formulation of new legal benchmarks and international collaboration (Wall, 2007).

The growth in cybercrime has been met with different legislative and policy responses by

governments and legal institutions. For instance, the Council of Europe Convention on Cybercrime provided a common ground for international cooperation in combating cybercrime in 2001. National jurisdictions, like the United States and the European Union, have enacted laws that specifically target several forms of cybercrime and have also formed agencies to deal with threats to cybersecurity. Despite these steps, issues still exist in balancing the law enforcement needs with the protection of individuals' private rights, and efficient collaboration between countries (Kerr, Cybercrime Law and Policy. In Cambridge Handbook of Surveillance Law. , 2018).

Improved technology in surveillance includes CCTV, facial recognition, and location tracking, which changed the game. Enhanced its application to issues of crime prevention, investigation, and general public safety. Besides, AI and big data analytics combined with AI-powered surveillance systems have greatly enhanced their capabilities for more exact monitoring and data analysis (Technolog).

Surveillance technology has huge implications for privacy. Some researchers argue that the enhanced ability to monitor the individual infringes on liberty and can result in power abuse. According to Solove (2007), control over these kinds of surveillance can be very thorny. Recently, attempts have been made to implement legal regimes that would set rules for collecting, storing, and using data. Examples include the General Data Protection Regulation of the EU and the different laws on privacy enforced in the US. However, some question the sufficiency of these regulations in light of rapidly evolving technology.

AI technologies have been swiftly placed center stage for integration into practices pertaining to law enforcement, such as predictive policing, facial recognition, and risk assessment tools. AI has the potential to enhance efficiency and effectiveness in policing by analysing massive datasets to find patterns that might not turn up under traditional analysis. However, the role of AI in policing also gives rise to concerns about bias, transparency, and accountability.

This does bring out a wave of difficult ethical and legal issues when artificial intelligence is used in criminal justice. Biased training data and algorithms can continue prejudiced practices while at the same time being instrumental in continuing further injustices in decision-making in law enforcement. Adding to that, the opacity and levelling of the algorithmic playing field with the use of black-box AI tools, these AI elements bite down harder on the contestations that can be made about the fairness of due process. In addition, this is going to establish a need

for guidelines to be developed and oversight mechanisms to be built that ensure the responsible and ethical use of these AI technologies.

RESEARCH METHODOLOGY

Approach: This paper will apply a qualitative methodology in its research.

Data Collection: The data shall be collected from the review of the existing literature, case studies, articles, statutes of criminal law, and technology.

On these subjects, analysis for qualitative data is done using thematic analysis, and quantitative data is analyzed using statistical methods in order to bring out the key trends and insights.

RESEARCH OBJECTIVES

1. To analyze the impact of technological advancements on the detection, investigation, and prosecution of crimes. To identify the benefits and challenges associated with the use of technology in criminal law.

2. To evaluate the legal and ethical implications of using digital evidence in court proceedings.

3. To explore future trends and potential developments in the integration of technology into the criminal justice system.

HISTORICAL BACKGROUND

The history of criminal law in India can be traced back to ancient times, during the empires of Maurya and Gupta, when policing was primarily in the hands of locals. There were far-reaching changes under British rule, particularly by the Police Act of 1861, laying the basis for modern policing in India. The problems facing the police force of India in the early post-independent period were manifold, as the methods were archaic, and it had turned corrupt, with limited resources[2].

The term “forensics” originates from the Latin word “forensis,” meaning “before the forum.”

[2] Vkeel. (n.d.). *The role of modern technology in modern law enforcement in India | Vkeel - Legal blog*. Vkeel.com. https://www.vkeel.com/legal-blog/the-role-of-modern-technology-in-modern-law-enforcement-in-india

This concept dates back to Roman times, where criminal charges were presented before a public forum, and cases were decided based on the quality of arguments and delivery. Modern forensics involves using scientific and investigative techniques to gather and analyse evidence for criminal cases, playing a crucial role in uncovering unknown aspects of a case.

The field of digital forensics began to take shape with the rise of personal computers in the 1980s, necessitating methods to investigate computer-related crimes. The earliest forms of digital forensics emerged in the 1970s, primarily involving mainframes and minicomputers. As personal computers became more prevalent, digital forensics expanded to include the analysis of computer systems and the recovery of evidence, continually evolving to keep pace with technological advancements.

CURRENT TECHNOLOGICAL DEVELOPMENT

The digital influences on the judicial system of India have changed legal processes and operations drastically. The e-Courts Mission Project, one of the most essential projects concerned with the digitization of case administration and judicial procedures, endeavours to have a uniform computerized environment in every court, from trial courts to the Supreme Court. It facilitates online filing of cases by litigants, solicitors, and judges, provides case information and electronic updates, hence fastening the process of justice and improving its access.

1. DIGITAL EVIDENCE

The world of digital evidence has been an interesting journey characterized by massive technological improvements and an increasing centrality in the criminal justice processes. Here:

- **Early Days (1980s-1990s):**

Origins: Digital forensics gained its shape during the mid-1980s when the personal computer became common in many homes, parallel to the rise in crime using computers[3].

[3] Champlain College Online. (2024, February 8). The evolution of digital forensics. *https://online.champlain.edu/blog/evolution-digital-forensics*.https://online.champlain.edu/blog/evolution-digital-forensics

Early Problems: The first advances were involved with learning how to gather and seize digital evidence without altering it.

- **Standardization and Expansion (2000s):**

Plagiarism on the Rise: The explosion in the use of the internet made plagiarism easy. Digital forensics was needed to catch those myriad criminals.

Development of Protocols: Law enforcement first started developing predetermined protocols and forensic labs specifically for and to perform investigations on digital evidence[2].

- **Modern Era (2010s-Present):**

Advanced Tools: Advanced forensic software and tools development have completely overhauled the collection and analysis of digital evidence[4].

Diverse Sources: Coupled with this, flows of digital evidence now include items from smartphones, cloud computing, and social media.

Legal and Ethical Considerations: On this note, it has been noted that digital evidence has raised important legal and ethical issues, in particular, matters concerning privacy and feasibilities of such evidence use in a court of law.

This evolution is characterized by the development of the growing complexity and significance of digital evidence in solving crimes and ensuring justice.

The judgment of Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2019) is one of the important decisions of the Supreme Court of India concerning the admissibility of electronic evidence. While delivering the judgment on 14th July, 2020, it has been reiterated that a certificate under Section 65B(4) of the Indian Evidence Act, 1872 (Stephen, 1872), is mandatory for an electronic record to be admissible as secondary evidence[5].

[4] *New Approaches to Digital Evidence Acquisition and Analysis | National Institute of Justice*. (n.d.). National Institute of Justice. https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis

[5] Ansari, M. A. (2021, September 28). Arjun Panditrao Khotkar case: The Story of Electronic Evidence so far. *Legal Wires*. https://legal-wires.com/columns/arjun-panditrao-khotkar-case-the-story-of-electronic-evidence-so-far/

It was a case of rejecting nomination papers filed after the scheduled closing time of nomination in an election process, bringing on record proof in the form of video recordings. The court held that without the certificate under Section 65B(4), such electronic evidence could not be admitted.

The judgment thus reiterated the principles laid down by the earlier judgment in the Anvar P.V. v. P.K. Basheer (Anvar P.V. v. P.K. Basheer , 2014) case and elaborated that any electronic record should the adhere to certain requirements provided under the law to ensure its authenticity and reliability[6].

FORNESIC DEVELOPMENT

a. NGS (Next-Generation Sequencing):

NGS represents the most developed DNA analysis technology in the present world, which permits, simultaneously, the analysis of hundreds of genetic markers, incredibly increasing depth and accuracy in forensic analysis. This technique of NGS has already been applied to complicated cases of remains identification in mass disasters or cold cases, enabling a more complete profile of genetics. In a very prominent case in Kern County, California, NGS was instrumental in connecting the suspect to a double homicide and had the potential to forever change the face of forensic science.

b. Investigative Genetic Genealogy (IGG):

IGG is an emerging forensic investigative methodology that combines the conventional DNA analysis process with genealogical research—it works by tracing family trees in order to narrow down the identity of a suspect. This procedure has been integral to cracking high-profile, cold cases like that of the Golden State Killer by way of suspect identification using distant relatives.

c. Biometric Identification:

Facial Recognition Technology:

[6] Editor_4. (2021, June 7). *The decision in Arjun Panditrao: Admissibility of electronic evidence in India continues to face hurdles | SCC Times*. SCC Times. https://www.scconline.com/blog/post/2021/06/07/electronic-evidence-2/

Facial recognition systems have become more accurate and reliable due to advancements in AI and machine learning. These systems are used in surveillance and identification of suspects from crowded places and at security checkpoints for identification verification.

Fingerprint Analysis:

Magnetic Fingerprinting: This method uses magnetic powders to perfect the prints in most surfaces, thereby improving fingerprint analysis.

Laser Ablation: This is one of the methods of removing surface contaminants using lasers, hence making latent fingerprints visible and easy to analyse.

CYBER CRIME

Cybercrime refers to illegal activities conducted through a computer medium, wherein computers, networks, and the Internet are primarily involved. Cybercrimes work by exploiting vulnerabilities in software, hardware, or human behaviour to result in illegal transactions of data, destruction of systems, or alteration of information for various malicious intentions. Unlike the conventional aspects of crimes, cybercriminals operate from anywhere, often crossing international borders and jurisdictional constraints[7].

Types of Cybercrime

Cybercrime is a very wide term. It includes:

Hacking: Unauthorized access to computer systems to steal, destroy, or change data.

Phishing: Fraudulent activity to acquire sensitive information. This will usually take the form of an email scam where the perpetrator is posing as someone trustworthy.

Ransomware: Malicious software aimed at encrypting data of a prospective victim, requiring them to pay some amount of money before the data is released.

[7] Money, B. (n.d.). Understanding Cybercrime: the threats, challenges, and emerging trends of the digital age. *https://www.brightmoney.co/learn/understanding-cybercrime-the-threats-challenges-and-emerging-trends-of-the-digital-age*. https://www.brightmoney.co/learn/understanding-cybercrime-the-threats-challenges-and-emerging-trends-of-the-digital-age

Identity Theft: Stealing personal information for committing fraud or other crimes.

Cyberstalking: harassment or stalking of individuals via the Internet.

Increasing Prevalence in the Digital Age - The digital age has seen a manifold rise in cybercrime through the combination of several factors:

More Connectivity: The rise in internet-enabled devices increased the attack surface for cybercriminals. With more devices online, there were greater avenues for exploitation.

Technology Advancements: The rapid technological advancement in areas like IoT, artificial intelligence, and cloud computing has opened up new vulnerabilities. The methods of cybercriminals are updated continuously to leverage these technologies.

Legal Frameworks

National and International Legal Frameworks: A number of national and international legal frameworks have been put in place in the war against cybercrime. These range from legislations and treaties to collaborative efforts at both the regional and global levels with respect to how to deal with the challenges of harmonization of legal response and international cooperation.

National Laws: So far, many nations around the world have drawn certain laws to deal with cybercrime. For example, there is the Computer Fraud and Abuse Act in the United States and the General Data Protection Regulation in the European Union, with provisions that deal with data breaches.

International Treaties: One of the most famous international treaties may be the Budapest Convention on Cybercrime; it created a comprehensive framework for combating cybercrime by way of promoting international cooperation and harmonizing national laws in dealing effectively with cybercrime.

Cooperative Efforts: Organizations such as INTERPOL and the United Nations Office on Drugs and Crime facilitate international cooperation through initiatives and working groups devoted to the issue of cybercrime.

Significant Cases

Notable cases of cybercrime: Outlining some notable cases of cybercrime can make a difference in explaining the effect and intricacy of such crimes on criminal law.

The Morris Worm, 1988, was one of the earliest reported cyberattacks, which paralysed thousands of computers and exposed the weakness of networked systems.

The Melissa Virus, 1999, was a fast-moving virus sent via email that substantially damaged and caused financial loss. It brought to the fore the requirement for effective measures of cybersecurity.

Operation Shrouded Horizon, 2015: This was an international operation that dismantled a large cybercriminal forum, underpinning the point about cooperation across borders in fighting cybercrime.[8]

Yahoo Data Breach, 2013-2014: Among the largest data breaches ever, this affected several billion user accounts and involved serious legal and financial consequences.

WannaCry Ransomware Attack, 2017: This worldwide ransomware attack affected hundreds of thousands of computers across more than 150 countries, quite vividly representing the potential of cyberattack-related devastation.

ARTIFICIAL INTELLIGENCE AND MACHINE

Applications in Criminal Justice: Artificial intelligence in collaboration emerges the criminal justice system with the useful needs. Video analysis: Through AI, the algorithms can identify the people and actions within the video based on criminal activity and public safety. DNA analysis: AI helped analyze the DNA evidence; this is highly accurate and faster. Gunshot detection: AI systems can quickly zero in on a gunshot to prepare the response of the law enforcement officers. Crime predictive analysis: The predictive models will make the allocation of resources in policing efficient[9].

[8] Major cases. (n.d.). *https://www.fbi.gov/investigate/cyber/major-cases*.
[9] *Using artificial intelligence to address criminal justice needs | National Institute of Justice*. (n.d.). National Institute of Justice. https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs

Pros and Cons:

Pros:

Efficiency: AI, in an application way, reduces the time taken for the process and replaces it with machine-man work. Accuracy: A More accurate machine learning model in analyzing the data than a human brain. Cost-Effective: AI is pretty much cost-effective in an investigation. Biases and Ethical Concerns: Data Bias: Since AI uses data from the past, it carries the same bias as it. Transparency: Only a few AI algorithms are transparent.

Fairness: Equitable outcomes should be ensured.

Accountability: Legal frameworks should deal with questions of responsibility[10].

Regulatory Challenges:

Privacy: Weighing the benefits of AI use against privacy concerns.

Legal Standards: Courts must adjust to AI-made evidence.

Education: Legal professionals must understand AI technologies.

Integration of Technology in the Courtroom:

Online Filing Systems:

Traditional making of legal documents involved paperwork; hence, delay and inefficiency.

Nowadays, it allows the process of online filing through digital platforms; thus less dependence on paper works is involved.

It allows quicker submissions, lessens the administrative load, and increases accessibility to litigants.

[10] *Artificial Intelligence in the Criminal Justice System: Demystifying Artificial Intelligence, its Applications, and Potential Risks | National Institute of Justice*. (n.d.). National Institute of Justice. https://nij.ojp.gov/library/publications/artificial-intelligence-criminal-justice-system-demystifying-artificial.

Digital Case Management Systems:

They allow for one-stop access to case information, schedules, and documents.

Judges, Lawyers, and all those connected with the case can prepare more effectively for the hearings and avoid mere dependence on the paper files.

Structured case management, better collaboration, and access from anywhere are the benefits that come with it. Electronic Evidence Presentation:

Multimedia facilities make it easy and effective to make presentations in court :

AV Aids: Projectors, screens, and interactive displays improve communication.

Digital Presentations: Lawyers are better able to present their evidence with visual aids more effectively.

Interactive Presentations: The emphasis on key points and annotations engages jurors and judges.

Impact on Trials:

Efficiency:

Technology makes all administration work smoother, reducing delays and paperwork.

Everything will move smoothly in the court, which benefits the judges, lawyers, and litigants.

Accessibility:

Video conferencing will help litigants appear remotely, accepting access to justice.

Previously, it was impossible for a litigant to join court, but virtually the system will be more inclusive.

Integrity of documents:

Digital archives would maintain the integrity of the case records.

Lesser risk of loss or tampering than in physical files

Communication:

Video conferencing will facilitate the virtual courtroom.

Safe online platforms will help communication to remain smooth between the parties.

Future Trends:

Augmented Reality (AR):

AR overlays digital information on physical spaces within the courtrooms.

Advertisements for better visualizations, presentations of pieces of evidence, and enhancing jury understanding.

Advanced Video Conferencing:

Video quality improved with the interactive features changing remote hearings.

Real-time collaboration, virtual witness testimonies are standard.

Blockchain for Evidence Management:

Blockchain for the evidence, securing it, making it tamper- proof, and transparent in management.

Chain of custody and authenticity verification in the process of legal proceedings[11].

Data Collection and Surveillance

Mass surveillance—today's technology makes it possible to gather data from an array of sources, from cameras to social media to the interception of communications.

[11] Shokeen, M., Sharma, V., & Department of law, University Institute of legal studies, Chandigarh University Gharaun Punjab, India. (2023). Artificial intelligence and criminal justice system in India: A crtical study. In *International Journal of Law, Policy and Social Review* (Issue 4, pp. 156–162) [Journal-article]. https://www.lawjournals.net.

Protection of Privacy: There needs to be a balance between concern for public safety and the respect for individual privacy rights.

Legislative Oversight: Adoption of robust legislation that sets controls on surveillance practices is central to ensuring the protection of citizens' privacy.

Biometric Data and Identification

Facial Recognition: Extensively in use in security, but it tends to cause privacy concerns. Misuse leads to false positives and invasion of privacy.

DNA Databases: Forensic use has to be balanced with the rights to privacy.

Consent: Proper mechanisms of consent must be developed for collection of biometric data.

Data Retention and Access:

Retention Periods: What duration should they be retained? The longer the retention period, the greater are the risks.

Access Control: Only authorized staff should have access to prevent any misuse.

Encryption: Keeping the stored data secure so that, in case of a breach, the privacy is still intact.

Emerging Technologies:

IoT—Internet of Things: Devices collecting personal data, and therefore, the privacy policies should focus on IoT.

Health Tech: Privacy concerns related to wearables, health apps, and medical records.

Smart Cities: Efficiency in urban functioning should be balanced with the concerns of citizens' rights to privacy

RECOMMENDATION

Clear Policies:

Policies: There should be well spelled out policymakers on the use of technology in criminal

justice. These should deal with privacy protection, ethical considerations, and the responsible deployment of technology.

Reconciliation Act: Policymakers need to balance between effective law implementation and protection of individual rights. Policies should be made which outline permissible ways for the use of technology, respecting the privacy.

Training and Education:

Legal Professionals: Legal professionals must be trained to know the subtleties of technology. This includes digital evidence, data privacy laws, and courtroom technology.

Constant Education: Technologies change very fast. There will be training to keep up with changing technologies and new best practices.

Collaboration:

Multidisciplinary Approach: There should be collaboration among technologists, legal experts, policymakers, and people in law enforcement. Each one brings expertise that is needed to provide all the perspectives necessary.

Design and Implementation: Allow technologists and legal experts to design effective solutions. Ensure that policymakers work to ensure the designs align with legal frameworks.

Public Awareness:

Education Campaigns: Educate the public on new criminal justice technologies. Inform the public of their purpose, benefits, and safeguards.

Building Trust: Transparency generates trust. Public awareness reduces scepticism and builds cooperation.

How technology impacts legal outcomes over time:

Benefits of Legal Innovation:

Increased Productivity: AI automates repetitive tasks to make time for strategic work by lawyers.

Improved Service to Clients: AI tools make service streamlined, increasing access to resources, all the while putting less stress on the client.

Costs Reduced: Even with the upfront costs, AI can reduce overhead costs—allowing firms to adopt more technology1.

Challenges:

Job Displacement: While automation may reduce some roles, this can actually improve the overall efficiency.

Client Confidentiality: Safety of AI tools and compliance with regulations have to be taken care of by the firms.

Implementation Costs: Large upfront costs can be a deterrent to smaller firms.

Opacity: AI conclusions can be impenetrable, hence, complicating legal decision-making[12].

Key Trends and Advances:

Generative AI: This technology can read reams of legal precedents and arguments very fast.

Cloud Computing: Improves the accessibility and collaboration of law firms by easier information storing and processing on remote servers, delivering real-time insights, and democratizing technology for smaller firms.

Automation and AI: Contract review, due diligence, legal analytics, e-discovery, and predictive analytics get drastically streamlined.

Future Outlook:

The impact that AI will have if it continues to evolve the way it does, will be what shapes the legal process.

Ethics have to equate with innovation.

[12] Legal innovation and AI. (n.d.). *https://www.americanbar.org/groups/law_practice/resources/law-technology-today/2024/legal-innovation-and-ai-risks-and-opportunities/*.

While machine learning can augment strategy, logic, creativity, and empathy in lawyers, it will not replace the latter[13].

How technology folds into criminal law, therefore, requires that there should be some balance and ethical considerations in the collection of evidence and its analysis. Thus:

DNA Databases: These are databases of genetic profiles used to identify suspects or solve cold cases. However, since it involves genetic information, there are privacy concerns.

Digital Evidence: Data from smartphones, computers, and social media play a very important role in any investigation process. Still, access to this information must be in line with the privacy laws that safeguard the rights of the people.

Predictive Policing:

Data Analytics, Machine Learning: Algorithms predict future hotspots based on analysis of historical crime data. While much effective, they have to be transparent and devoid of bias.

Ethical Challenges: Making sure predictive policing does not disproportionately affect any certain communities or perpetuate other biases is important.

Surveillance Technologies:

Cameras and Facial Recognition: Surveillance cameras and facial recognition systems enhance the safety of public places but at the same time, a balance between security and privacy has to be maintained.

License Plate Recognition: It is used for tracing vehicles, hence assisting law enforcement. At the same time, it increases the issues associated with mass surveillance.

Courtroom Technology:

Virtual Hearings: A digital courtroom offers remote participation, increasing efficiency and access.

[13] *The promise and peril of AI legal services to equalize justice*. (2023, March 14). Harvard Journal of Law & Technology. https://jolt.law.harvard.edu/digest/the-promise-and-peril-of-ai-legal-services-to-equalize-justice.

Electronic Filing: This eases the burden of case management but requires stringent cybersecurity measures.

Challenges and Considerations:

Privacy: It is important to protect citizens' privacy while using surveillance technology. Laws should be defined for permissible limits.

Bias: Algorithms must, in particular, be audited so that they would not be biased. Proper training of the law enforcers regarding ethical AI use is observed to be necessary.

Security of data: Digital evidence integrity and secure storage are very critical.

SUGGESTION

Interdisciplinary Collaboration:

Convene frequent meetings among legal scholars, technologists, and policymakers. Indeed, the foregoing regular dialogues can accomplish informed decisions and effective regulations.

Joint research tasks, workshops, and conferences would assist in bridging the gap between law and technology.

Ethical AI Education:

Practice-oriented training on AI, machine learning, and data analytics should be imparted to practicing legal professionals and students of law. More specifically, understanding the limitations of the technology itself and its probable biases is quite important.

Courses in ethics while dealing with technology can find a place in the syllabus of law schools.

Public Awareness Campaigns:

Educate citizens about their rights and what technology does for criminal justice.

Make surveillance practices and data collection transparent.

International Cooperation:

Technology knows no borders. Cooperate with other countries to address issues of common concern, such as cybercrime, data sharing across borders, or extradition.

Adaptive Legislation:

Laws have to keep up with technology. Update them regularly to address new issues.

Open up flexible, responsive legislative procedures to enable the legislative process to keep pace with change.

CONCLUSION

It is true that the interplay between criminal law and technology raises a number of pressing concerns for the development of legal frameworks dealing with the complexity brought about by rapid technological development. Indeed, new technologies do not only bring new opportunities to commit crimes but also innovative instruments of crime prevention, detection, and prosecution. It follows, therefore, that this research underlines the need for a proactive approach to law—a flexible legal regime that will be in a position to rise to new challenges emerging from technologies without compromising justice and human rights.

On the other hand, equal to the challenges, there is a collaborative approach in updating privacy protection, management of digital evidence, and regulation of new technologies—areas that demand continuous stakeholders' dialogue between policymakers, legal professionals, technologists, and civil society with regard to developing and implementing regulations for efficiency and deference toward constitutional safeguards.

There is also an acute need for the training of law enforcement agencies and the legal fraternity, so that they may be better equipped to deal with digital evidence and cybercrime issues. Bigger investments in research and development are further needed to keep pace with any threats likely to arise and to utilize technological advancements for the betterment of society.

Ultimately, a thoughtful, adaptive legal framework will enhance the criminal justice system's ability to respond to challenges and opportunities brought about by technology. By

incentivizing and protecting innovation that safeguards the rights of persons, it can help call into being a safer, fairer society in the digital age.

REFERENCES

- Artificial intelligence and criminal justice system in India: A crtical study (lawjournals.net). (n.d.). *Artificial Intelligence and Criminal Justice System in India: A Crtical Study (lawjournals.net)*

- *The Advancement of technology in deterring Crime: Benefits and difficulties for Indian law enforcement*. (n.d.). https://www.legalserviceindia.com/legal/article-8576-the-advancement-of-technology-in-deterring-crime-benefits-and-difficulties-for-indian-law-enforcement.html

- *Cybercrime And its Challenge in The Digital Era*. (n.d.). https://www.legalserviceindia.com/legal/article-10425-cybercrime-and-its-challenge-in-the-digital-era.html

- Https://www.exterro.com/resources/blog/digital-forensics-reimagined-elevating-Indias-police-departments-with-AI-into-2024-and-beyond. (n.d.). *https://www.exterro.com/resources/blog/digital-forensics-reimagined-elevating-indias-police-departments-with-ai-into-2024-and-beyond*.

- The role of modern technology in modern law enforcement in India | Vkeel - Legal blog. (n.d.). *The Role of Modern Technology in Modern Law Enforcement in India | Vkeel - Legal Blog* The Role Of Modern Technology In Modern Law Enforcement In India | Vkeel - Legal Blog

- Important Cases on Information Technology Act, 2000 (lawyersclubindia.com). (n.d.). *Important Cases on Information Technology Act, 2000 (lawyersclubindia.com)*

- Garg, R. (2023, October 25). *Cyber crime laws in India - iPleaders*. iPleaders. https://blog.ipleaders.in/cyber-crime-laws-in-india/

- Bose, A. (2021, November 12). *Overview of famous cyber crime cases that target people instead of money - iPleaders*. iPleaders. https://blog.ipleaders.in/overview-of-famous-cyber-crime-cases-that-target-people-instead-of-money

- Forensics, O. (2024, May 16). *What is Digital Forensics?* Oxygen Forensics. https://oxygenforensics.com/en/resources/what-is-digital-forensics