LEGAL AMENITY LAW JOURNAL – ISSN 3107-9148

Volume 1 Issue 1 September – October 2025

ROLE OF TECHNOLOGY IN PREVENTING CRIMES

By- Aayushhi Siingh

PhD 3rd year Shri Krishna University, Chhattisgarh, MP

ABSTRACT

Technology plays an indispensable role in examining and preventing crime, offering innovative solutions to rising criminal activities. Advancement in technology aligns with a legal regime that focuses on public safety, due diligence, and the systematic administration of justice. This research paper explores the multifaceted role of technology in preventing crimes[1]. Technological tools such as surveillance systems, biometric identification, and data analytics have become essential components in preventing crimes. Predictive policing that enables artificial intelligence (AI) and machine learning allows law enforcement agencies to examine and analyse historical crime data, which identifies potential crime hotspots, enabling precautionary intervention. Cyber tools and digital fore nsics aid in investigating complicated crimes such as cyber fraud, identity theft, and data breaches, ensuring that digital evidence is collected and preserved by legal standards. This paper focuses on contributing to the ongoing discourse on technology-enabled crime prevention that offers valuable insights for policymakers, practitioners, researchers, and communities endeavouring to create safer and more resilient societies in the technological world. The paper analytically scrutinizes the dual role of technology as both a facilitator of public safety and a probable threat to individual rights. It helps in balancing the need for a balanced legal framework, which ensures the responsibility of technology in preventing crimes while protecting fundamental rights enshrined in constitutional and international law.

INTRODUCTION

In the modern world, technology has revolutionized crime prevention. From the adoption of surveillance technologies to the use of predictive analytics and forensic science advancements, technology plays a pivotal role in responding to criminal activities. These technological innovations empower communities to actively participate in crime prevention actively, fostering collaborative partnerships between citizens and law enforcement.

The development of technology has changed every aspect of human existence, including

[1] McQuade, Sam. "Technology-Enabled Crime, Policing and Security." *The Journal of Technology Studies*, vol. 32, no. 1, Winter 2006, pp. 32–42. https://www.jstor.org/stable/43603623

crime prevention. With the advancement of digital tools, data analytics, and communication platforms, law enforcement agencies have gained unmatched capabilities. These innovations have not only empowered law enforcement but also communities, encouraging active participation in crime prevention and fostering collaborative partnerships between citizens and law enforcement entities.

The changing dynamic of technology is directly linked to changes in society, which include urbanization, globalization, and the emergence of new types of criminal behaviour.

Expansion of population and traditional policing methods pose challenges in addressing complex and dynamic patterns of criminal offences. Historically, Law enforcement surveillance of the community is very important, as it plays a crucial role in preventing crime and enhancing the detection of crime. Community is kept safe by using law enforcement to prevent crime.

A HISTORICAL PERSPECTIVE

Ancient era:

The historical form of crime prevention technology was community based and mechanical which used to use tools like primitive locks, keys and powerful buildings and guard animals' torches used in places like Mesopotamia and Egypt, But in places like Ancient Rome an old and cruel way, named The vigiles like torturing, whistles and trained animals for patrolling the streets at night.

Medieval era:

In Europe, especially in medieval times, preventing crime was primarily community-based. Citizens used to create a "hue and cry' ' to raise alarms to capture the criminal, especially in places like England. Night guards patrolled the streets with horns, lanterns, and shaming in public to scare off wrongdoers. Ten households gathered in groups and were responsible for law-abiding behaviour.

1. **Era of rise in scientific policing and forensics**: In the 17th to 19th centuries, there was a rise in scientific policing, and society accepted the revolutionary changes in technology for preventing crime.
2. **Sir Robert Peel established the London Metropolitan Police (1829)**:- This helps in patrolling, professionalism, and the use of uniforms to create an environment where people

fear committing crimes. Use of Nightsticks, whistles, and printed wanted posters. Police adopt systematic patrolling, patrol lags, and use of shift-based organization.

3. **Advancement of Forensic Science Fingerprints:** ancient civilizations used fingerprints for business and scientific purposes, which began in the late 19th Century. In 1892, Sir Francis Galton developed the first classification system. In the year 1835, Scotland Yard used bullet comparison in solving cases of murder. The analysis of gunpowder residue and tool marks has become more standardized over time. Alphonse Bertillon's anthropometry system was the first. In the late 1800s, mugshots became standard police procedure, marking the beginning of visual surveillance and profiling.

The 20th Century-

The 20th Century witnessed a transformative growth in crime prevention technology, particularly with the advent of modern communication technologies. Police departments began using these technologies in the 1920s-1930s, enabling them to receive dispatches and respond promptly. The introduction of vehicles further enhanced mobility, allowing officers to reach crime scenes more quickly. In the mid-20th Century, closed-circuit television (CCTV), which was first used in the UK in the 1960s, became the most widely used in big cities. It is used in public places, which provides evidence for investigation. Also, wiretapping and recording devices which is critical for the investigation of organized crime, especially in cases of drug trafficking and corruption.

In the mid-century, fingerprinting became crucial, and FBO developed an identification division in 1924, which by the 1940s, had millions of fingerprint records. In the 1980s, Automated fingerprint identification systems (AFIS) emerged, which allowed for a quicker and more precise way of matching fingerprints. In the year 1967, NCIC was established, which was a computerized index of criminal justice information. It was the first technology used to centralize data for nationwide crime prevention.

From the 1990s to the early 2000s, there was an advent of internet and digital technology in the late 20th Century., As the advancement of new digital threats develops, cybercrime units are tasked with tackling hacking, identity theft, and online fraud. National security and intelligence agencies faced virus attacks on their data; therefore, firewalls, antivirus software, and encryption became critical tools. The most crucial development in forensic science was DNA profiling. In 1984, Sir Alec Jeffreys established the first DNA profiling technique. In the year 1986, Colin Pitchfork was convicted of criminal murder. CODIS(Combined DNA

Index System) was launched in the USA in 1998, enabling law enforcement to match DNA samples across jurisdictions, revolutionizing the ability to solve crimes and prevent repeat offenses. The NYPD implemented a geographical information system in the 1990s, which used data-driven analysis to identify crime hot spots, enabling better resource allocation and patrol planning

21st Century Era :-

In the 21st Century, technology has continued to evolve and take center stage in crime prevention. From facial recognition and AI-driven analytics to mobile safety apps and cyber forensics, modern law enforcement and communities are leveraging these technological advancements to prevent and combat crime.

Development of high-density CCTV networks in cities worldwide. Also, advanced smart cameras include behavior analysis models to detect suspicious patterns like hidden weapons and changeable behavior, which can effectively enhance surveillance to identify threats. Automated license plate recognition (ALPR) recognizes law enforcement, like flagging stolen or wanted vehicles automatically. It helps to enable rapid detection and alerts in traffic areas.

Drones are used for significant events or remote areas. For example, during India's Kumbh Mela, drones help manage massive crowds and detect irregularities. Drones-based patrols provide flexible aerial supervision. Equipping officers with wearable cameras that enhance transparency reduces complaints and provides authentic evidence for investigation and trials. This helps in building public trust and discouraging wrongdoing.

Policies that are predictive in another technology in preventing crimes by analyzing historical crime data, geographical trends, and social patterns, and algorithms that can be used to predict and suggest an ideal arrangement of public resources. For instance, programs like CompStat (Comparative Statistics) used by the Newyork police department help law enforcement officials identify crime hotspots, which determine patterns, and implement strategic interventions. Predictive models allow for better allocation of resources, which includes response times and increased visibility of law enforcement in high areas. Big data analytics and machine learning tools help in identifying the relationship between socio- economic factors and criminal behaviour. It enables reactive policing, which aims at diminishing the leading causes of crime.

As times have changed, personally, financially, and governmentally, information has shifted to online. Cybercrime has become one of the most challenging in the 21st Century. It includes

offences such as identity theft, online fraud, hacking, data breaches, and cyberbullying.

Sophisticated cybersecurity technologies were developed to curb crimes. Governments and companies invest in cybersecurity infrastructure to prevent financial losses and threats to national security.

Artificial Intelligence (AI) and various machine learning techniques are increasingly being used to find irregularities in network behavior and to identify potential security threats. These systems can learn from past attacks to adapt to new threats, which improves potency over time.

Biometric technology has been revolutionary in identification verification and access control, offering an authentic and secure way of preventing unauthorized access to sensitive locations or systems. Fingerprint scanners, iris recognition, facial recognition, and voice authentication which is used in both public and private sectors. Automated fingerprint identification systems (AFIS) enable the fast identification of suspects who link individuals to crime scenes. For border security and immigration control, biometric passports and facial recognition enhance security. These systems not only prevent crimes like identity fraud but also help in criminal investigations by providing undeniable proof of a person's presence at a particular time and place.

The incorporation of mobile and wearable technologies into policing transforms how officers should perform their duties. Police officers should perform their duties. Police officers use body-worn cameras to record interactions with the public, which enhances transparency and accountability. BWCs are used to reduce incidents of misconduct and improve the community. Mobile data terminals in patrol cars and handheld devices allow officers to access criminal databases, file reports, and communicate with headquarters. GPS enables devices to help track officers' movements, ensuring a structured arrangement. The use of real- time centres (RTCCs) involve aggregating data from different sources. That includes CCTV,911 calls, license plate readers, and social media, which provides a comprehensive view of public safety in the specified area.

Social media platforms have been a platform that can be used either as a boon or a bane against crimes. Criminals use social media for various illicit motives, including trafficking, fraud, and recruitment. Law enforcement agencies also use platforms to gather intelligence, monitor public sentiment, and engage with the people. Police monitor potential threats, find organized criminal activity, and prevent crimes before they happen. To build trust with the public, the department uses social media to share information, request assistance, and build trust with the

public. Also, educational content and digital campaigns aid in raising awareness about the prevention of crime, cybersecurity, and emergencies.

Forensic science has been enhanced by technology, such as DNA analysis, which can be efficiently conducted with high accuracy. Portable DNA analyzers and automated fingerprint identification systems accelerate investigations that could reduce case backlogs. Digital forensics involves extracting data from electronic devices like computers, smartphones, and tablets, which plays a vital role in solving cybercrimes and traditional crimes alike. Files that are deleted, encrypted communications, and geolocation data that could provide critical evidence in criminal trials. Forensic ballistics, chemical analysis, and trace evidence analysis benefit from technological innovations that increase the accuracy of forensic analysis.

CASE LAWS- EVOLUTION OF TECHNOLOGY

In the old case of **Kharak Singh (1963**), it was first laid that the right to privacy was not acknowledged as a fundamental right. It also laid the basic foundation for subsequent cases, which strengthened the right to privacy as essential and should be restricted. In the case **o**f **PUCL vs. Union of India (1997),** it sets guidelines under the Indian Telegraph Act for lawful telephone tapping, according to Article 19(1)(a) of the Indian Constitution. Helps to access information about political candidates[2]. In another case of **Suhas Katti vs. Tamil Nadu (Chennai, 2004)[3],** it was the first cyber crime conviction in India under Section 67 of the IT Act for obscene online messages. It introduced electronic evidence under Section 65B of the Evidence Act. And the court allowed a private techno-legal consultant's certified data from Yahoo. It emphasizes the importance of upholding dignity and respect in the digital space. In the case of **Abhinav Gupta Vs. State of Haryana (2008**)[4], It involves theft of confidential and copyright data from a former employer. The court transferred the amount to hack within the meaning of Section 66 IT Act, and bail was rejected. **Tomaso Bruno & Anr. Vs. State of U.P. (2015, Supreme Court**),[5] In this case, CCTV footage was admitted as primary evidence to place the accused at the scene of the crime. Evidence through CCTV qualifies under section

[2] People's Union for Civil Liberties v Union of India (1997) 1 SCC 301; AIR 1997 SC 568

[3] State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004, Additional Chief Metropolitan Magistrate, Egmore, Madras (Nov. 5, 2004

[4] Abhinav Gupta v. State of Haryana, High Court of Punjab & Haryana, Faridabad, Crl. M.P. No. 438 of 2008 (Apr. 25, 2008

[5] AIR 2015 SC (SUPP) 412

65 of the Evidence Act. In the case of **Lalit Kumari v. State of U.P. (2014[6])**. The SC emphasizes the mandatory registration of First Information Reports (F.I.R) for cognizable offenses, which include cyber-crimes. This case highlights the importance of liability in cybercrime investigations. In the case **of Shreya Singhal Vs Union of India**,[7] the SC struck down Section 66A of the IT Act on free speech under Section 19(1)(a) of the Constitution. It sets limits on arbitrary surveillance of online content. In one of the landmark cases of Justice. **K.S. Puttaswamy (Retd.) Vs. Union of India (2017),** the Supreme Court declares the right to privacy a fundamental right under Article 21. In this case, the Supreme Court challenges the constitutionality of Adhaar because it violates the right to privacy established by the constitution bench under the Constitution of India.

RECENT INNOVATIONS OF TECHNOLOGY

Internet of things

Urban infrastructure has been merged into the Internet of Things, such as bright lighting, connecting traffic cameras, gunshot detectors, and emergency communication systems. For example, ShotSpotter uses acoustic technology to locate gunfire, which enables immediate police response to save lives. In the case of emergency management systems, the use of AI, GPS, and mobile networks helps coordinate responses that manage evacuations and alerts. All this helps in preventing secondary crimes like looting, which enhances circumstantial awareness.

Significant privacy concern

Collection of data and widespread surveillance raises significant privacy concerns. Facial recognition, location tracking, and internet monitoring occur without individual consent. Policies must be transparent, and mechanisms must strike a balance between public safety and civil liberties.

Biasness in data

Sometimes, bias in historical data could lead to over policing of marginalized communities. Addressing these issues requires diverse data sets, regular audits, and the inclusion of social scientists in designing the system.

[6] Lalita Kumari v. Government of U.P. & Ors., (2014) 2 SCC 1 (India 2014)
[7] Shreya Singhal v. Union of India, AIR 2015 SC 1523 (India 2015)

Legal framework

Updated laws are regulated by AI in policing, defining digital evidence and establishing accountability for the misuse of surveillance and data tools.

International Cooperation and Policies

Crime has a very extended scope, and it was necessary to make international policies to curb crime. The integration of policy frameworks, bilateral and multilateral treaties, and global technology standards is essential in crime.

GLOBAL INSTITUTIONS FACILTATING TECHNOLOGY- DRIVEN CRIME

INTERPOL

The International Criminal Police Organization (INTERPOL) is the leading entity in the coordination of global police cooperation. It operates in securing a global police communication system known as 1-24/7 that connects 195 member countries. The technological initiatives include forensic tools and threat assessments. International law enforcement, such as red notices, identifies and arrests suspects across borders[8].

EUROPOL

The European Union Agency for Law Enforcement Cooperation (Europol) supports member states in the prevention and fighting of organized crime, terrorism, and cybercrime. It establishes the European Cybercrime Centre (EC3), which specializes in coordinating digital investigations across borders. It uses different tools to secure information exchange, such as SIENA. EIS (Europol Information System) for cross-border data analysis and AP (Analysis Projects) for identifying different patterns in drug trafficking, child exploitation, and fraud[9].

[8] .Zagayno, Mikhail R. "Interpol Activities and Artificial Intelligence Issues." *Sociopolitical Sciences*, vol. 15, no. 3, July 2025, pp. 93–99. Interpol Activities and Artificial Intelligence Issues | Yur-VAK

[9] .Biriukov, R. M. "The Institutional Development of the European Police Agency (Europol) after the Adoption of the Europol Convention." *Uzhhorod National University Herald. Series Law*, vol. 4, no. 87, March 2025, pp. 193–199. (PDF) The institutional development of the European police agency (Europol) after the adoption of the Europol convention

United Nations Office on Drugs and Crime (UNODC)

The UNODC promotes global standards in the prevention of crime. It supports the development of national capabilities in the use of technology and helps in implementing international legal frameworks like the UN Convention against Transnational Organized Crime (UNTOC) and the UN Convention against Corruption (UNCAC)[10]

TO CURB INTERNATIONAL CRIME, TECHNOLOGY USED:

Biometric databases and identity verification

Biometrics include facial recognition, fingerprinting, and iris scans for immigration control, extradition procedures, and fugitive tracking. INTERPOL's AFIS (Automated Fingerprint Identification System) enables member states to submit and have query fingerprints across different areas. Biometric shares agreements like the Five Eyes alliance (Australia, Canada, New Zealand, the UK, and the U.S that accelerate identification in terrorism and human trafficking cases.

Cyber Forensics and Cybercrime Units

Cybercrime units across the globe use forensic software, network analysers, and malware detection tools to investigate international cyber incidents. Tools like X-rays forensics, Encase, and Cellebrite support digital investigations by reconstructing deleted files, tracing cryptocurrency transactions, and communications. International collaboration includes joint cyber task forces hosted by Europol, cross-border search warrants, and digital. Cloud data reviews under MLATs (mutual legal assistance treaties). Real-time intelligence shared through encrypted platforms. Countries adopt AI-driven threat analysis, automated border surveillance, and satellite imaging to track illegal activities like smuggling and piracy. For example, NATO uses satellite and radar data to detect unlawful migration and maritime crime. The Schengen Information System (SIS) enables police in Europe to monitor individuals who enter the Schengen Zone.

[10] United Nations Office on Drugs and Crime (UNODC). "Meeting the Challenge: A Guide to United Nations Counterterrorism Activities." Jan. 1, 2012, pp. 125–129. United Nations Office on Drugs and Crime (UNODC) from Meeting the Challenge: A Guide to United Nations Counterterrorism Activities on JSTOR

CASE STUDIES-INTERNATIONAL TECH-DRIVEN PREVENTION OF CRIME

Operation Trojan Shield (Encro Chat /Anom)

In the landmark case, law enforcement agencies from the U.S., E.U., Australia, and others ran a secret operation called Operation Trojan Shield, wherein criminals used a fake encrypted messaging app, ANOM. This data led to over 800 arrests globally[11].

The International Child Sexual Exploitation (ICSE) database, maintained by INTERPOL, uses image recognition and AI to identify victims and track offenders across borders.

Countries that participate upload digital evidence that helps link cases and identify repeat offenders on a global platform[12].

SUGGESTION FOR IMPROVEMENT

Interoperability and Enhancing data sharing:

Unified crime Databases: develop international and regional interoperable databases that law enforcement agencies can securely access, such as fingerprints and facial recognition.

Protocols need to be standardized: Creating global standards for formatting and transmitting digital evidence that ensures data shared between jurisdictions is admissible in court.

API Integration Between Agencies: Building APIs to link national and international systems for real-time information sharing Upgradation of Artificial Intelligence and Predictive Analytics AI models need to be trained on different datasets to reduce racial, gender, or socio-economic bias in policing predictions.

Models Behavioral Predictive**:** Machine learning is used to analyze unusual online behaviour or movements in public areas to detect potential threats early (e.g., pre-crime indicators in cyberbullying and radicalization).

---

[11] On the Admissibility of Evidence Obtained via Operation Trojan Shield (ANOM): A Review of BGH 1 Strafsenat Urt. v. 09.01.2025 – 1 StR 5424." *Journal of Criminal Law and Criminology*, vol. 117, no. 1, January 2025, pp. 101–120 (PDF) On the admissibility of evidence obtained via Operation Trojan Shield (ANOM). A Review of BGH (1. Strafsenat), Urt. v. 09.01.2025 - 1 StR 54/24

[12] Child Sexual Exploitation Material: Motivations for Use and Implications for Deterrence, Treatment, and Prevention." In *Sexual Crime and the Internet*, August 2025, pp. 15–34. https://doi.org/10.1007/978-3-031-95844-1_2.

Humans should be in the loop: Ensuring that humans supervise AI tools to improve decision-making and avoid false positives.

Advancements in Biometric and identification verification tools: Combining fingerprints, facial recognition, voice, and gait analysis for accurate suspect identification.

Decentralized identity systems: Use of blockchain to store biometric credentials securely, which allows verification of identification without exposing sensitive personal data.

Investment in Smart Surveillance and Lot Integration: Upgradation of public surveillance systems with AI to detect weapons, unusual behaviour, or known criminals. Installment of sensors, drones, and automated lighting in high crime areas that trigger alerts based on sound. Uses of integrated sensors in traffic lights, public transport, and utilities to track activities and support law enforcement.

Expansion of International Cybersecurity Cooperation: Establishment of regional hubs for collaboration on threat intelligence, dark web investigations, and rapid response to cross-border cyberattacks.

Cyber threat Simulation platforms: Creating shared platforms for countries to test and improve incident response through simulated attacks.

Public-Private Cyber Alliances**:** Collaborating between governments and tech companies to detect, trace, and shut down cybercriminal infrastructure.

Increment on public access**:** Anonymous Platforms that allow citizens to report crimes. Allowing communities access to specific data alerts to support neighborhood policing and launching virtual reality (VR) apps and games that educate children and vulnerable groups about fraud, abuse, and cyberbullying.

Strengthening of legal and Ethnic governance: Creating legislation to regulate the use of AI in surveillance and predictive policing, including transparency, accountability, and redress mechanisms, and encouraging global pacts on ethical AI deployment in law enforcement and surveillance for the protection of civil liberties and ensuring that new law enforcement is developed with built-in privacy and data protection.

Training of law enforcement and judiciary: Regularly training police officers, investigators, and judges in new technologies, digital forensics, and cybersecurity protocols. AI ethics, data governance, and civil rights education are included in training programs for law enforcement.

Uses ODF Simulation Skill development to prepare officers for complex scenarios like hostage negotiations, cybercrime incidents, or digital evidence handling.

Development of crime prevention-oriented innovation labs**:** Hosting of invitations which bring coders together, designers, and criminologists to prototype new tools for the safety of the public. Research on technologies like quantum computing, neuromorphic chips, and synthetic data in the prevention of crime. Creating a real-world testing machine to see the authenticity of new surveillance, AI, and forensic tools.

CONCLUSION

Technology is an essential tool in the modern fight against crime. Technological innovations have potentially helped in preventing crime. Surveillance systems, facial recognition, and data analytics raise crucial questions about balancing between security and individual rights. There must be proper supervision to see probable abuse. As we move forward, a balanced approach is needed, which is a combination of old technology innovations with human judgment, transparency, and ethical frameworks.