Minnesota Journal of Business Law and Entrepreneurship

Volume 2026, No. 2

ISSN: 1540-3270

Interoperable Criminal Justice Systems and Financial Governance: Comparative Analysis of India, USA, UK and Europol

[1]Ms. Medha Singh, [2]Dr. Kanchal Gupta

Ph.D. Scholar, School of Law, UPES Dehradun

Sr. Associate Professor, School of Law, UPES Dehradun

Abstract

The Crime and Criminal Tracking Network and Systems CCTNS is one of India's largest digital governance initiatives aimed at modernising policing and criminal justice administration through integrated information infrastructure. Implemented under the National e-Governance Plan and coordinated by the National Crime Records Bureau, CCTNS digitally connects police stations, crime records repositories, and related criminal justice institutions to facilitate real-time information exchange, investigation support, and citizen-centric services. Existing literature has predominantly examined CCTNS from technological and policing perspectives; however, limited scholarship addresses its implications as a public digital infrastructure project within the domains of financial governance. This paper analyses CCTNS through the lens of financial governance, regulatory compliance, and international cooperation. It conceptualises CCTNS as a long-term public technology asset requiring sustained investment in infrastructure, cybersecurity, data management, interoperability, and lifecycle maintenance. The study evaluates financial issues relating to public expenditure, procurement frameworks, vendor accountability, implementation risks, service-level obligations, and technology governance. It further examines the transition of CCTNS from a standalone policing platform to an integrated component of the Inter-operable Criminal Justice System ICJS, thereby expanding its operational and financial significance. The paper also situates CCTNS within global criminal information architectures by comparatively examining systems such as the United States' National Crime Information Centre NCIC, the United Kingdom's Police National Database PND, and Europol's Secure Information Exchange Network Application SIENA and internationally aligned governance frameworks, positioning it as a critical digital public infrastructure within contemporary criminal justice administration.

Keywords- CCTNS, Policing, Governance, Information, Criminal justice system CJS

Introduction

Information technology has become an indispensable component of contemporary policing and criminal justice systems. Across jurisdictions, law enforcement agencies increasingly rely on integrated information networks, centralized databases, and digital governance platforms to enhance crime prevention, investigation, inter-agency coordination, and service delivery. India's Crime and Criminal Tracking Network and Systems represents one of the most significant manifestations of this global transition towards digitally enabled policing. Introduced in 2009 under the National e-Governance Plan, CCTNS was conceptualised to modernise police administration, strengthen information sharing, and address structural inefficiencies in crime and criminal record management. The project emerged against the backdrop of increasing internal security concerns, particularly following the 26/11 Mumbai attacks, and sought to create a unified national platform for crime data management and criminal justice coordination. The Ministry of Home Affairs designated the National Crime Records Bureau as the nodal agency for implementation, with an initial approved outlay of approximately ₹2,000 crore for nationwide deployment.

This paper examines CCTNS as a complex information system from multiple angles. First, it delineates the technical architecture of CCTNS, describing the infrastructure, the data flow between local, state, and central components, and how CCTNS integrates with other systems such as ICJS , hereinafter referred to as the Inter-

operable Criminal Justice System, and specialized databases like e-Prisons. Understanding the architecture is crucial to appreciating how CCTNS functions as a backbone for policing data. Secondly, this paper reviews the implementation process across India, highlighting major milestones and the challenges faced. These challenges have been technical, such as ensuring connectivity in rural areas and migrating legacy data, administrative such as coordinating between central agencies, state police IT teams, and private vendors, and logistical such as training thousands of personnel, deploying hardware to remote locations. The solutions and strategies, from engaging System Integrators to establishing Project Management Units, also discuss as to illustrate how India managed an IT project of this scale in a federal structure. Third, an impact assessment evaluates how far CCTNS has achieved its goals. Its effect on day-to-day policing, crime tracking efficiency, the facilitation of inter-agency collaboration through data sharing, improvements in citizen-facing services like online complaint filing or police verification, and any contributions to transparency and accountability in policing, for instance, by digital audit trails of police work.

Finally, to contextualize CCTNS globally, the paper compares CCTNS with similar international criminal information systems. It looks at the USA's National Crime Information Centre, operational since 1967 as a centralized crime database; the UK's Police National Database, launched in 2011 to enable nationwide sharing of local police intelligence; and Europol's Secure Information Exchange Network Application SIENA, introduced to facilitate secure cross-border information exchange among European law enforcement agencies. This paper therefore analyses CCTNS as a public digital infrastructure project by examining its technical architecture, implementation trajectory, financial dimensions, and international interfaces. It argues that the long-term effectiveness of CCTNS depends not solely on technological integration but equally on sustainable financial governance, regulatory compliance, and internationally compatible operational frameworks.

Prior to CCTNS, India's crime and criminal records were largely maintained in fragmented and localised repositories, often manually or through limited standalone systems such as the Crime Criminal Information System CCIS and the Common Integrated Police Application CIPA. These systems lacked nationwide interoperability and restricted effective information exchange across jurisdictions. CCTNS sought to address these deficiencies by digitally linking police stations, state crime records bureaus, and national databases through a common software architecture and integrated communication framework. Beyond operational efficiency, this transition introduced new economic and governance dimensions relating to technology procurement, public-private implementation partnerships, data governance, and digital compliance obligations.[1]

The architecture of CCTNS is a multilayered system designed to network thousands of police establishments while accommodating India's federal governance of police data. At its heart lies the Core Application Software, the CAS, which is the primary software framework for entering, storing, and retrieving crime and criminal data. CAS exists in two variants: CAS-State and CAS-Centre. CAS-State is deployed in each State/Union Territory and contains the core functionalities common to policing needs across India. These include modules for First Information Report FIR registration, investigation tracking, evidence, case diary, chargesheet preparation, criminal record search, crime analytics and reporting, and a basic citizen interface for complaint registration and service requests. [2]

CAS-Centre, hosted by NCRB, serves to receive and aggregate data from all states into a National Database and to provide central services such as nationwide search queries and data analytics for policy-making. Essentially, CAS-Centre acts as the brain of the system at the national level, while CAS-State is the workhorse at the ground level police stations.[3]

---

[1] Comptroller and Auditor General of India, *Report on Information Systems Audit of Crime and Criminal Tracking Network and Systems (CCTNS)* https://cag.gov.in/uploads/icisa_it_reports/7db9b967001ebeec572b498754f61af4.pdf accessed 25 May 2026.

[2] Ibid n.1

[3] e-Committee, Supreme Court of India, *Inter-Operable Criminal Justice System (ICJS)* https://ecommitteesci.gov.in/icjs/accessed 25 May 2026.

CCTNS infrastructure is distributed across police station-level hardware, State Data Centres and a National Data Centre. Each police station and higher police office is equipped with computers, connectivity equipment, and often a local server or storage for caching. These local nodes access the CAS-State application over a network. The CAS-State servers are typically located at the SDC of the respective state, which is a secure centralized IT facility managed by the state often under State IT department or NIC. All police stations in a state connect to the SDC via an intranet or secure network to use the application and database hosted there. Meanwhile, the NDC, managed by NCRB, often using the National Informatics Centre's data centre facilities hosts CAS-Centre and the national database that syncs with state databases. In early years, the communication between states and the centre involved periodic data replication and the states would upload their FIR and arrest data to CAS-Centre on a scheduled or real-time basis, thereby populating the central repository. This design choice of a distributed database with central aggregation was driven by the need to allow states to operate independently yet contribute to and draw from a unified national information pool. [4]

Implementing CCTNS across India's vast policing apparatus was a formidable undertaking. The project's rollout spanned more than a decade, involving multiple phases and adjustments. Key milestones in the implementation process can be chronologically outlined as follows:

Project Initiation and Design. The Cabinet Committee on Economic Affairs approved CCTNS in June 2009 with a ₹2000 crore budget. NCRB was appointed the central coordinating agency and immediately set about hiring a Software Development Agency SDAWipro Ltd was contracted to develop CAS Centre and CAS State and to serve as the central development and support partner. Simultaneously, states signed Memoranda of Understanding MoU with MHA to take part in CCTNS e.g., Uttar Pradesh signed in Oct 2009. Each state was to set up a State Mission Team and a State Project Management Unit to oversee implementation at their level. Pilot projects were identified in some states such as Kerala, Assam, UP were early pilots to test the system in a few police stations.

By 2011, the core application was developed and handed to states. CAS Centre went live at NCRB on a pilot basis. System Integrators SIs were procured in each state to deploy the hardware, network, and customize CAS State for local requirements. Training content was developed and "train the trainer" programs began at NCRB and State Police Academies. The initial project plan was aggressive many states aimed to achieve a "Go-Live" by 2012. However, in practice, this timeline proved optimistic. Some states had pre-existing systems or higher technical capacity and moved faster. Others faced procurement delays or technical hurdles.[5][6]

By 2012, it was clear the project needed more time. The deadline was extended to March 2015. During this period, many states achieved significant progress: procurement of over 20,000 computers and peripherals, establishment of connectivity in thousands of locations, and migration of legacy data like digitizing old FIRs from registers. States followed a phased approach often starting with a few pilot police stations, then a district, then statewide. Key milestones included completing site preparation ensuring power supply, UPS, etc. at stations, hardware installation, and CAS deployment. For example, Kerala reported finishing its pilot by 2013 and gradually scaling up. By March 2015, NCRB reported that about 75% of police stations were entering data digitally in at least one module of CCTNS. The progress, however, was uneven: some states like Tamil Nadu and Telangana achieved near 100% operationalization early, whereas others like Bihar and the Northeast states lagged due to infrastructure issues. The central government responded by increasing support dispatching teams to assist lagging states, organizing frequent video-conferences to troubleshoot issues, and providing additional funds for connectivity e.g., satellite links where terrestrial networks hadn't reached.

By 2016, with most states on board, NCRB launched the Digital Police Portal in Aug 2017 as a central online interface for both police and citizens. This portal signified that CCTNS had enough critical mass of data to be useful at a national level. Police users via this portal could do national searches or use analytical tools; citizens

[4] Ibid n. 1

[5] *ETGovernment*, 'CCTNS 2.0 ICJS Meghraj Cloud: Revolutionizing India's Criminal Justice System with CCTNS 2.0 and ICJS Integration' https://government.economictimes.indiatimes.com/blog/revolutionizing-indias-criminal-justice-system-with-cctns-20-and-icjs-integration/123422358 accessed 25 May 2026.

[6] Ibid n.3

could avail services online, indicating that many states had integrated their citizen services like tenant verification, complaint filing with the CCTNS backend. In these years, the emphasis shifted from mere data entry to data utilization. NCRB started building specialized search tools for instance, a tool to match missing persons with found/unidentified persons across states by searching names, physical descriptors on CCTNS data. The National Database of Sexual Offenders NDSO was rolled out in 2018, drawing data from CCTNS to list convicted sexual offenders accessible to law enforcement. These initiatives were both milestones in terms of new capabilities and incentives for states to keep improving their data quality.[7]

By mid-2019, the project claimed over 90% of police stations were entering 100% FIRs through CCTNS. Efforts concentrated on the last mil eonnecting the few hundred remaining police posts, often remote outposts. The involvement of BharatNet as mentioned earlier was crucial here; by July 2021, NCRB stated CCTNS application was deployed in 16,276 police stations 100% of the target, with 97% of them having connectivity. Also notable is that by 2020–21, many old paper processes had been digitized: NCRB indicated that the proportion of FIRs directly generated through CCTNS and thus available digitally to courts rose from 70% in 2019 to 85% in 2021. An important milestone was the CAS Centre 5.0 go-live in February 2021. This was essentially the deployment of an updated version of the central system, and an agreement with C-DAC for ongoing maintenance of CAS State applications. The upgrade improved system stability and paved the way for new features like faster search, improved user interface, etc..

In recent years, focus has been on deepening the system CCTNS 2.0 and integrating across the justice system ICJS Phase II. By August 2025, the system had fully covered all intended police stations over 17,700 and was entering a maturity phase. The Phase II of ICJS was sanctioned to run from 2022–23 with an aim for seamless data exchange and adoption of analytics and AI in policing. New modules and complementary systems were introduced, such as the Investigation Tracking Tool for Sexual Offences ITSSO which leverages CCTNS data to monitor investigation timelines in rape cases. Thus, implementation has moved beyond just installation to iterative enhancement and policy-driven use of the system.[8]

Network connectivity was a persistent problem. Many police stations, especially in rural or hilly terrains, initially had no data connectivity; this required coordinating with telecom providers, using VSATs, and later BharatNet. Even with connectivity, ensuring uptime and bandwidth for a web-based system was difficult, it impacted user confidence when the system would lag or go down. Another challenge was data migration and digitization. States had decades of crime records on paper and in legacy systems like CCIS/CIPA databases. Converting these into digital form scanning, or entering key fields was time-consuming. Poor quality of historical data, missing records, and lack of standardization meant that when migrated into CCTNS, there were errors and inconsistencies. The ET Government analysis in 2025 observed that heterogeneous data across states different versions of CAS or custom modules complicated creating a centralized clean dataset, delaying rollout in places and reducing end-user trust when information was incomplete. To mitigate this, NCRB set data standardization drives, and some states outsourced data entry of old cases. However, the audit trails show some states chose to only migrate certain critical data and left old records in physical form due to resource constraints.

The project required coordination between central authority NCRB/MHA and 35 States/UTs, each with its own police hierarchy and home department. Setting up effective governance structures was key. Many states formed a high-level Empowered Committee under the Chief Secretary or Home Secretary to oversee CCTNS. Still, issues arose like timely fund release, procurement bottlenecks some SIs struggled to procure hardware meeting specifications, causing delays. There were also vendor management issues, different states had different SIs TCS, Polaris, NIIT, etc., aside from Wipro's central role. Their performance varied; if an SI underperformed, state systems suffered. States like Bihar initially lagged, reportedly due to issues with the selected vendor and challenges in personnel training, but later made rapid progress after focused attention and support.

[7] Ibid n.2
[8] Ibid n.1

Logistical and Human Resource Challenges: Training over 150,000 police personnel in basic computer usage and the specifics of CCTNS was a massive task. Early on, many frontline police showed resistance or lack of interest, the extra work of data entry was seen as a burden, especially when staff shortages meant the same officer had to do both field work and computer work. To address this, capacity building programs were ramped up. NCRB and BPR&D developed standardized training modules and even e-learning for continuous training. Over time, computer literacy improved and younger personnel naturally adapted to the system. However, even as late as 2025, usage patterns indicated that many personnel only used basic features like FIR registration and not the advanced tools like analytics, search, or investigation modules. This under-utilization often stemmed from insufficient training depth and the enduring habit of doing things the old way. Top police leadership had to issue directives making CCTNS entry mandatory for all FIRs and prisoner data, etc., to enforce compliance. Logistically, maintaining equipment especially in adverse environments was also challenging, UPS batteries, printers, biometric devices needed maintenance and consumables, which required annual budgets and vendor support that were not always timely.[9]

Getting the police leadership to buy into data sharing and transparency was another subtle challenge. Historically, Indian police stations maintained their own registers and sometimes were reluctant to share "their" data for reasons ranging from inertia to concerns over misuse by other agencies. CCTNS, by design, makes data visible across the state and country to authorized users, reducing a station's exclusive control over information. Overcoming this cultural challenge involved sensitization that shared data would benefit all and directives that mandated information updating. The anecdote of how Haryana police started seeing value when a criminal involved in a series of robberies was caught only because another state's FIR was found on CCTNS is a classic example shared in police trainings, which helped change attitudes toward collaborative data use.

In spite of these challenges, the strategies employed to facilitate deployment included strong project monitoring NCRB had a Central Project Management Unit and each state had a State PMU; progress was monitored through monthly reports and dashboard indicators, and iterative problem-solving where connectivity was poor, offline solutions were given; where software had bugs, updates were released. The central funding was also structured to incentivize performance, funds were released in tranches upon achieving milestones like 30% stations live, then 70%, etc. This pushed states to accelerate implementation. Additionally, peer learning was encouraged: states that did well like Karnataka or Telangana presented their best practices in national workshops so others could emulate for instance, Telangana's use of Mobile Data Terminals in patrol vehicles integrated with CCTNS inspired other states to consider similar extensions. By 2023, CCTNS implementation could be declared largely successful in terms of rollout, virtually all police establishments in India were on the network. The few challenges that remained had shifted in nature: from setting up the system to optimizing its use. The presence of CCTNS in everyday policing had become routine, and the focus moved to quality of data and leveraging the system for outcomes crime prevention, investigation speed, etc. rather than just data entry compliance.[10]

Impact Assessment of CCTNS

With over a decade of implementation, CCTNS has had multifaceted impacts on policing in India. This section evaluates the outcomes in key domains: 1. Efficiency and Effectiveness in Policing Operations: One of the primary goals of CCTNS was to enhance the efficiency of police at the police station level. There is evidence that CCTNS has indeed reduced procedural delays and made information retrieval much faster. For instance, prior to computerization, getting the details of an old case or a person's criminal history could take days of rummaging through paper registers or sending written requests to other districts/states. Now, an officer can pull up the criminal record of a suspect within seconds by querying the national database. The KPMG case study on CCTNS noted that over 40 million records were digitized FIRs, charge-sheets, etc., dramatically cutting down information access times and preventing data loss. In practical terms, this means when a person is detained, the police can quickly

[9] Ibid n.5
[10] Ibid n.5

check if the person is wanted elsewhere or has past offenses, leading to more informed and timely investigative decisions. As another example, stolen vehicles: CCTNS has a centralized stolen vehicle database, so any vehicle intercepted can be instantly checked; recovery of stolen automobiles across state borders has improved due to this shared data though exact statistics are not published, qualitative reporting by officers confirm many "NCIC-style" success stories in India now. CCTNS has also improved police workflow management. Registration of FIRs on the system enforces standardized formats and mandatory fields, which enhances completeness of information. Important investigation milestones like arrest memos, case diary notes, forensic results can be recorded and tracked, which helps supervisory officers monitor progress. A concrete impact is seen with specialized modules like the Investigation Tracking for Sexual Offences ITSSO. ITSSO, built on top of CCTNS, uses the data of FIR and charge-sheet dates to monitor compliance with the 60-day investigation deadline in rape cases as mandated by law. This module automatically flags delays to senior officers, thereby instilling greater accountability in investigators to complete investigations promptly. NCRB's data indicates that since ITSSO's rollout, a higher percentage of such cases are being completed within the prescribed period, showcasing how digital monitoring drives performance though again, exact percentage improvements are proprietary data, the MHA has praised states which achieved 100% compliance using ITSSO. Another measure of efficiency is reduction in redundant work. CCTNS's mantra of "enter data once, use many times" has cut duplication. For instance, when an FIR is registered, multiple reports to senior officers, to NCRB for crime stats, to courts can be generated from that single entry, rather than re-writing the same information in different registers or forms. According to NCRB, this has freed up police manpower from clerical tasks to more core policing tasks. Some states have attempted to quantify this: Maharashtra police estimated that digitization through CCTNS reduced the time spent on preparing routine reports by 50%, as the software could auto-generate monthly crime statements and charge-sheet abstracts. 2. Crime Tracking and Investigation Outcomes: By enabling inter-state connectivity, CCTNS has had a significant impact on crime tracking, especially crimes that involve mobility of offenders organized crime, vehicle theft, kidnapping, etc.. Police now regularly use the national search to identify patterns, e.g., a series of similar robberies in different cities can be linked if the description of modus operandi or suspects matches, something that was far more difficult earlier. The Cri-MAC Crime Multi Agency Centre, launched by NCRB in 2020, leverages the CCTNS database to share alerts on notorious interstate criminals and organized gangs. When one state flags an incident involving such criminals, an alert is broadcast to others. This has improved inter-state coordination; for example, a gang of dacoits operating across three states was apprehended after Cri-MAC alerts connected their activities, an outcome directly arising from CCTNS data sharing. Furthermore, specialized databases built on CCTNS data, like the National Database of Sexual Offenders NDSO, have improved tracking of repeat offenders. The NDSO launched in 2018 compiled identities of those convicted of sexual offenses across India around 1 lakh individuals. Police have used it in investigations to quickly shortlist suspects in cases like serial sexual offenses by checking if known offenders were present in the area. These tools were not imaginable without a national digital system. CCTNS has also started to facilitate data-driven policing and analytics. While at a nascent stage, some states are using the data for crime mapping and trend analysis. For example, Delhi Police uses CCTNS data to generate heatmaps of crime occurrences, which inform patrol deployments though Delhi has its own e-police system integrated with CCTNS. Some insights such as identifying hot-spots of crime, recidivism rates, etc., are being extracted more easily. The use of analytics and AI is explicitly mentioned as an aim of ICJS Phase II and CCTNS 2.0, anticipating predictive policing applications. Already, in a few pilot projects, machine learning algorithms have been tested on CCTNS data to identify crime patterns e.g., series of burglaries with similar characteristics. The impact of such analytics is yet to be fully realized, but the infrastructure now exists for it, marking a departure from intuition-driven policing to evidence-based policing. CCTNS's integration with other criminal justice pillars via ICJS has gradually improved collaboration. A notable impact is quicker communication between police and courts. Previously, after an FIR was filed, the police had to send physical copies to magistrate courts; now many states have e-FIR modules where the FIR is electronically shared with the court system, reducing delays in court cognizance.[11] The Supreme Court's e-Committee noted that through ICJS, FIR metadata from CCTNS is accessible to all High Courts and subordinate courts, allowing judges to know case details without waiting for

[11] Ibid n.5

paper files. Similarly, the integration with e-Prisons means that police can, through CCTNS, get real-time information on under-trial prisoners or convicts useful when investigating jail contacts or when needing production warrants. The seamless exchange of data has improved timeliness; for example, if a prisoner is released on bail, the police station can be immediately notified via the system which helps them update surveillance lists, etc.. Another collaboration improvement is with forensic labs: using e-Forensics integration, police can digitally send forensic requisitions and track reports, reducing the lag in getting forensic results which often delayed investigations. While full integration is still ongoing, one can already see better coordination. An anecdotal impact: a police officer investigating a crime can now see on one screen the FIR police data, the charges filed once prosecutor updates e-Prosecution, whether the accused has other cases or has appeared in court courts data, and if the accused was in jail previously prisons data. This 360-degree view was not possible before and allows a more holistic approach to criminal justice. Additionally, central agencies like NIA or CBI, which have nationwide jurisdiction, now often use CCTNS as a starting point for information when taking over cases, they can quickly gather the local police data of a case from CCTNS rather than requesting physical files. One of the most visible impacts of CCTNS has been on citizen-facing police services. The project enabled the launch of online portals for citizens in every state sometimes called "Digital Police Citizen Portal", often accessible through the national Digital Police Portal as well. Citizens can now file certain types of complaints online e.g., report loss of documents or lodge non-cognizable complaints, request services like police clearance certificates or tenant verifications online, and even check the status of their FIR or complaint using these portals. For example, someone who applied for a character certificate can track on the portal whether the report has been prepared or not, bringing transparency and reducing the need to visit the police station repeatedly. In some states, online FIR registration for minor crimes has been enabled Delhi and Jharkhand allow online FIRs for theft of items below a certain value, etc., all feeding into CCTNS directly. The availability of these services 24/7 has improved public accessibility to the police, an oft-cited statistic is that 24/7 citizen service portals have been launched, leading to increased engagement and convenience. The uptake is notable; for instance, hundreds of thousands of tenants' verification requests are now processed through CCTNS portals annually across metro cities, which earlier required physical forms. This not only makes it easier for the public, but it also structures the data for police a verified tenants database can help in investigations. Transparency is another area of impact. With digital records, there is a reduced scope for tampering or "misplacing" files, an FIR once registered in CCTNS cannot be destroyed without leaving an electronic trail, which guards against malicious disappearance of complaints. Senior officers have real-time oversight of police station records. This has indirectly curbed some malpractices; for example, if an SHO Station House Officer was reluctant to register a case, a complainant can escalate to district authorities who can see the digital register and intervene. Some states have given the public limited access to certain data, e.g., lists of proclaimed offenders or missing persons are published online via the CCTNS portals, increasing transparency. In terms of accountability, digital systems log actions: who edited a file, when was a charge-sheet filed, etc. [12][13]This creates audit trails that internal vigilance departments can use to identify negligence or misconduct e.g., if an investigation was unduly delayed, one can check the timestamps in CCTNS to see periods of inactivity.[14] Moreover, CCTNS data contributes to better statistics and policy planning. NCRB's annual Crime in India report, which is a key transparency document on crime trends, has benefited from CCTNS, data collation is faster and likely more accurate because it's drawn from the live database. Policymakers use these statistics to allocate resources for example, seeing an increase in cyber-crimes in a state might prompt more cyber police stations. However, it is important to note some limitations in impact. [15]While CCTNS has largely digitized records, the degree to which

[12] Garg M, 'CCTNS 2.0 and ICJS Integration with Meghraj Cloud: Transforming India's Criminal Justice System' *ET Government* (21 August 2025) https://government.economictimes.indiatimes.com/blog/revolutionizing-indias-criminal-justice-system-with-cctns-20-and-icjs-integration/123422358 accessed 25 May 2026.

[13] Government of India, Ministry of Home Affairs, *Development of Tools for Mainstreaming Disaster Risk Reduction in Environment Sector – CCTNS Report* https://www.mha.gov.in/sites/default/files/IIPA-Report-CCTNS.pdf accessed 25 May 2026.

[14] Ibid n.13

[15] Government of India, Ministry of Home Affairs, *Digital Police – About Us*https://digitalpolice.gov.in/DigitalPolice/AboutUs accessed 25 May 2026.

it has improved conviction rates or reduced crime is complex and not solely attributable to the system. [16]Conviction rates depend on investigation quality and prosecution, CCTNS aids the process but doesn't itself investigate. Some critics point out that despite CCTNS, issues like low police-citizen ratios and skills deficit still hamper policing outcomes. There's also the issue of data quality, a system is only as good as the data entered. In initial years, many entries had errors misspelled names, incomplete addresses, etc. which could lead to missed matches or wrongful matches. Continuous data cleaning and validation efforts are needed. NCRB has recognized this and called for automated data quality checks and standardization across states as a future improvement. There's also the matter of privacy and misuse. As more data including biometrics, facial images, etc. gets aggregated, ensuring it's used only for legitimate purposes is an ongoing concern. The presence of audit logs and user authentication in CCTNS is intended to deter misuse, but ensuring all users adhere to the legal and ethical guidelines is a human factor beyond just the system's scope. [17]In sum, the impact of CCTNS on policing in India has been substantially positive in terms of efficiency gains, better information for decision-making, and service delivery improvements. [18]It has ushered in a new era of policing where digital evidence and records form the backbone of investigations and oversight. The interlinking of agencies fosters a more cohesive justice system. Citizens have started to see police as more accessible and accountable due in part to these technological changes. A senior police officer encapsulated it by saying that CCTNS and allied reforms are transforming Indian policing "from a paper-diaries era to a data-driven era," with decisions increasingly based on real-time information and trends rather than solely on an officer's personal knowledge. The next section will place these observations in perspective by comparing CCTNS with analogous systems abroad, which have their own set of impacts and challenges.[19]

International Perspective

Large-scale criminal information systems are critical components of law enforcement worldwide. Comparing CCTNS with international counterparts provides insight into different architectural choices and their consequences, as well as highlighting best practices that transcend borders. This section examines three systems: the National Crime Information Centre NCIC in the United States, the Police National Database PND in the United Kingdom, and Secure Information Exchange Network Application SIENA operated by Europol for EU member states. Each serves a similar fundamental purpose, sharing criminal justice information, but under different governmental and operational contexts.

United States: National Crime Information Centre NCIC

The NCIC is one of the oldest and most established law enforcement information systems in the world. Launched in 1967 and managed by the FBI's Criminal Justice Information Services Division, NCIC was conceived to assist in apprehending fugitives and recovering stolen property by providing a centralized database accessible

[16] Government of India, Ministry of Home Affairs, *Inter-Operable Criminal Justice System (ICJS)*https://www.mha.gov.in/en/commoncontent/inter-operable-criminal-justice-system-icjs accessed 25 May 2026.

[17] Government of India, Press Information Bureau, *Press Release* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2039059 accessed 25 May 2026.

[19] Ibid n.14

nationwide. Over time, its scope has expanded to cover a wide array of criminal justice data. NCIC is a centralized, national database system. [202122]

The FBI maintains the central host computer system historically a mainframe, now a robust server system at the CJIS facility originally in Washington, D.C., now in Clarksburg, West Virginia. This central system interfaces with each state through what are known as Control Terminal Agencies, typically the state police or state bureau of investigation computers which in turn connect to local law enforcement terminals. In essence, NCIC operates on a hub-and-spoke network: the FBI is the hub, and each state plus certain federal agencies and territories is a spoke that fans out to local agencies. Communication initially was via dedicated telecommunications lines; nowadays it runs over a secure internet-based CJIS network. The design is highly resilient and emphasizes immediate query response; even back in 2006, the average NCIC query took only 0.06 seconds, thanks to continual tech upgrades. NCIC's database is organized into multiple files as of 2017, it had 21 files, including 7 property files e.g., stolen vehicles, guns, etc. and 14 person files wanted persons, missing persons, known terrorists, sex offender registry, etc.. Additionally, NCIC provides access to the Interstate Identification Index III, which is essentially a pointer system to detailed criminal history records held by states rather than storing all criminal histories centrally, NCIC indexes them and retrieves from state repositories. This highlights an important aspect: NCIC is not just one database, but an integrated system of several databases and indices. Interoperability: NCIC achieves interoperability by being the common system that all agencies plug into. Over 94,000 law enforcement agencies in the U.S., from federal to local, have access to NCIC via their state connections. This universal access means any officer, say a city police officer or a border patrol agent, can run a query that goes against the national data. NCIC is also integrated with other federal systems. For example, it is linked with the National Instant Criminal Background Check System NICS for firearm purchase checks, and with the Terrorist Screening Centre TSC database post-9/11, terrorist watchlist records were included in NCIC. [23]It interfaces with motor vehicle registries via the NLETS network National Law Enforcement Telecommunications System which routes DMV data. Thus, an NCIC check on a license plate will simultaneously hit stolen vehicle file in NCIC and the state's vehicle registration via NLETS, giving a combined result.[24] The key to NCIC's interoperability success is the shared data standards and protocols established through FBI and the Advisory Policy Board which includes state representatives. They ensure that data entered by any agency meets certain quality and format, making nationwide sharing seamless. Effectiveness: NCIC is often cited as a backbone of American policing. Statistics illustrate its extensive use: by mid-2010s, NCIC was handling on the order of 14 million transactions per day. In 2016 alone, it processed over 2.4 billion queries by law enforcement. The system has been directly credited with countless "hits" that led to arrests. One example in FBI literature is the arrest of a murder suspect in Tennessee after a trooper ran a license plate check on NCIC and learned the car was stolen from a homicide victim in another state. Such instances are routine NCIC ensures that police nationwide are alerted if someone or something they encounter is flagged anywhere else in the country. NCIC's effectiveness also lies in officer safety: before approaching a vehicle or suspect, an officer can know if the person is wanted and potentially armed and dangerous. It acts as a silent partner in every traffic stop or investigative stop. Because NCIC has been around for decades, it benefitted from a culture of use every academy graduate in the US knows to "run it through NCIC." The compliance and participation by all agencies local agencies are required or strongly expected to enter records of stolen property or warrants into NCIC promptly mean the database's coverage is comprehensive. With 12 million active records by 2017, NCIC's breadth is enormous. In terms of maintenance and challenges, NCIC has undergone periodic

---

[20] Evidence2e-CODEX, *SIENA Workshop Documentation* https://evidence2e-codex.eu/p/d/2/d2-01e2eworkshop20190327panel5-siena-431.pdf accessed 25 May 2026.

[21] Federal Bureau of Investigation, Criminal Justice Information Services Division, *NCIC Record: 5.6 Million Queries in a Single Day* (15 February 2006) https://archives.fbi.gov/archives/news/stories/2006/february/ncic021506 accessed 25 May 2026.

[22] Federal Bureau of Investigation, Criminal Justice Information Services Division, *NCIC Turns 50* (27 January 2017) https://www.fbi.gov/news/stories/ncic-turns-50 accessed 25 May 2026.

[23] Federal Bureau of Investigation, *NCIC Record: 5.6 Million Queries in a Single Day*https://archives.fbi.gov/archives/news/stories/2006/february/ncic021506 accessed 25 May 2026.

[24] Ibid n.23

overhauls NCIC 2000 was a major upgrade introducing modern OS and capabilities like images for missing persons or fingerprints for unidentified persons. [2526]The next planned iteration, NCIC Third Generation N3G, aims to incorporate new user requirements and perhaps more advanced search e.g., better biometrics, free text search. One challenge NCIC faces is data quality and civil liberties concerns; there have been instances of erroneous entries leading to wrongful arrests false positives. To counter that, the FBI has stringent rules for record validation and periodic audits of participating agencies for compliance with NCIC policies. For CCTNS, NCIC offers a blueprint of sustained success through standardization, training, and continuous improvement. However, differences exist: NCIC operates in a federal system with a stronger central role FBI has authority to enforce standards compared to CCTNS where state police have more autonomy. NCIC also does not directly concern itself with citizen servicesit's purely law enforcement facing and thus does not have a public portal like CCTNS does. Another difference is NCIC's focus: it's heavily geared towards indexing and locating wanted, stolen, missing rather than being a full police case management system. CCTNS, conversely, covers the workflow of case management end-to-end at police stations. Thus, NCIC and CCTNS have overlapping goals but different scopes.[27]

United Kingdom: Police National Database PND

The UK's Police National Database PND was introduced in 2011 as a response to critical failures in sharing police intelligence across regional constabularies. The impetus was the Bichard Inquiry 2004 into the Soham murders[28], which found that information on the offender's past allegations held by some forces was not known to the hiring force a failure of sharing that had tragic consequences. The PND was envisioned to "provide a national intelligence overview from local data" by aggregating and making searchable the vast amount of police information held by the 43 police forces in England and Wales and other forces/ agencies in UK. Technical Structure: PND is essentially a national data store and search interface that collates selected information from all local police databases. UK police forces traditionally operate their own record management systems for crime, custody, intelligence, etc., and PND was built to pull data from these into one system. Technically, it can be seen as a centralized repository of replicated data. Over "230+ local databases" feed into PND, including records of crimes, custody, domestic abuse incidents, child protection information, etc., from each force. The data is loaded into PND on a scheduled basis some feeds might be near real-time, others daily/weekly. Once in PND, authorized users from any force can perform searches across the national dataset. The PND has advanced search capabilities not just text queries but also image searching facial images, and bulk search tools.[29] For example, an investigator can run a search on a name or phone number and find any records across the country that mention it. The system is designed with role-based access; sensitive intelligence is protected by need-to-know controls and audit logs as per a national Code of Practice.[30] Unlike NCIC, which is transaction-oriented each query hits the live data, PND is more analytics-orient edit builds an index of national data that can be mined. Interoperability: PND's main function is to enable interoperability among the UK's multiple police agencies, effectively breaking down the

[25] Federal Bureau of Investigation, *NCIC Turns 50* https://www.fbi.gov/news/stories/ncic-turns-50 accessed 25 May 2026.

[26] Federal Bureau of Investigation, *The FBI's National Crime Information Center*https://archives.fbi.gov/archives/news/testimony/the-fbis-national-crime-information-center accessed 25 May 2026.

[27] Ibid n.25

[28] Bain A and Sutton A, 'What Does the UK Police National Database Tell Us About the Future of Police Intelligence?' *Policing: A Journal of Policy and Practice*https://academic.oup.com/policing/article/doi/10.1093/police/paac074/6686660 accessed 25 May 2026.

[29] Home Office (UK), *Code of Practice on the Operation and Use of the Police National Database*https://assets.publishing.service.gov.uk/media/5a7b8841ed915d4147620fc5/9999102808.pdf accessed 25 May 2026.

[30] Home Office (UK), *Police National Database 1.5 Transformation Accounting Officer Assessment (12 September 2024)*https://www.gov.uk/government/publications/home-office-major-programmes-accounting-officer-assessments/12-september-2024-police-national-database-15-transformation-accounting-officer-assessment accessed 25 May 2026.

geographical silos that previously existed. It connects not just the 43 territorial forces of England & Wales but also agencies like the British Transport Police, Police Service of Northern Ireland, Police Scotland, and some national bodies National Crime Agency, etc.. By policy, PND doesn't replace local systems; instead, it supplements them. Each force continues to maintain its primary records, but also supplies to PND. One notable aspect is that PND is separate from the Police National Computer PNC. The PNC dating back to the 1970s holds criminal records convictions, wanted persons, vehicle ownership, etc. and is akin to NCIC in some ways. PND was created to focus on intelligence and operational information that may not meet the threshold of PNC. For example, local intelligence about a suspect like allegations, associates, or vehicles frequented would be on PND even if the person has no conviction hence not on PNC. In practice, officers might use both: PNC for criminal history, PND for broader intelligence including soft information. Effectiveness: The PND undoubtedly filled a vital gap in UK policing by enabling cross-force intelligence sharing. There have been numerous cases where PND searches have aided investigations: for instance, finding a suspect who committed crimes in different regions by linking reports, or safeguarding vulnerable people by identifying repeat patterns across areas. The Policing Journal study includes examples: one where an image from social media was run through PND's facial search and matched to a known person from another force's database, leading to a quick arrest. Another where a threat to clergy in one area was recognized as a person flagged in another area via PND. [31]These anecdotes show PND's value in practice: connecting dots that would otherwise remain isolated.[32] However, PND's effectiveness has been tempered by varying usage. Research indicates that different forces use PND with different frequency and depth. Some smaller forces rely on it heavily because they lack their own sophisticated systems, whereas a few larger forces were initially slower to integrate PND queries into their routine perhaps due to confidence in their own intel systems or concerns over data security. There were also cultural challenges early resistance where officers felt sharing "their" intelligence undermined control or were wary of data misuse by others. Over time, these attitudes have improved, especially as success stories accumulate and governance frameworks reassure data protection. The UK Home Office and HM Inspectorate reports emphasize consistent use and have set expectations for forces to contribute and consult PND in relevant investigations. Another challenge has been technical aging.[33] A 2021 National Audit Office report noted that some of PND's infrastructure was nearing end-of-life, impacting service quality. The Home Office decided to keep PND running as a standalone system until at least 2031 but to invest in it for stability. This is partly because a larger project, the Law Enforcement Data Service LEDS, is planned to eventually unify PNC and PND into one modern system. Meanwhile, enhancements like better data analytics and integrating PND with other databases e.g., terrorism databases, or linking with child protection systems have been ongoing. From CCTNS's perspective, PND offers lessons on the human factors of adoption. The need for consistent training and promotion of the system's value was highlighted PND's usage correlates with forces where leadership mandated its use and provided proper training. CCTNS similarly requires continuous buy-in and showcasing of successes to encourage full usage beyond just mandatory data entry. Also, PND's model of aggregating from local systems is somewhat akin to how CCTNS aggregates state data. Both faced the complexity of normalizing data from heterogeneous sources. The UK overcame some of it by defining common data formats and a Code of Practice to ensure forces supply quality data. India's CCTNS, by providing a common software CAS, had an advantage in standardization from the start, but where states diverged or added custom fields, similar normalization issues appear at the national level.[34]

[31] Home Office (UK), *Code of Practice on the Operation and Use of the Police National Database*https://assets.publishing.service.gov.uk/media/5a7b8841ed915d4147620fc5/9999102808.pdf accessed 25 May 2026.

[32] Kirkpatrick MD, 'Testimony on the National Crime Information Center (NCIC)' (Statement before the United States Senate, 13 November 2003).

[33] Ibid n. 29

[34] Ibid n. 30

Europol: Secure Information Exchange Network Application SIENA

Unlike NCIC or PND, which are primarily databases, SIENA is a communication system facilitating exchange of information between law enforcement agencies across different countries. Europol, the European Union's law enforcement cooperation agency, operates SIENA to enable swift and secure sharing of crime-related information among EU member states and some non-EU partners. SIENA became operational in 2009 and has since become the default channel for bilateral/multilateral exchanges of police information in Europe. Technical Structure: SIENA is essentially a secure messaging application with additional features to support law enforcement needs. It functions much like an encrypted email or ticketing system: a user e.g., a national Europol unit officer can compose a message, attach files intelligence reports, documents, images, etc., and send to one or multiple recipients other countries' Europol national units or Europol analysts. All messages are tagged with handling codes that specify how the information can be used for intelligence only, or usable in court, etc.. SIENA ensures these communications are encrypted and logged. It can be accessed via a web interface, and also integrated with national systems via web services. For example, a country could link its case management system to SIENA so that an investigator can send out a request to other countries from within their local system, and it travels through SIENA. One key feature is that SIENA supports multimedia and large files, although for very large files Europol has a separate tool Large File Exchange which is not fully integrated into SIENA as of now.[35] SIENA is built to handle multi-agency connectivity; not only police, but customs, border, and even judicial authorities in some contexts can have access, under the "multi-agency approach" encouraged by Europol. Crucially, SIENA is not a public-facing system at all; it operates on Europol's secure network and each user is vetted. It's not a "Google" of criminal data, but rather a pipeline to ask and answer questions across borders. Interoperability: SIENA's raison d'être is interoperability across sovereign jurisdictions. Before SIENA, police cooperation in Europe was slower, often involving Interpol or diplomatic channels. With SIENA, if say the French police want information on a suspect who might be hiding in Spain, they can send a SIENA message to Spain's authorities within minutes, and vice versa. As of mid-2020s, over 50 countries and some 3,500 competent authorities this includes sub-agencies like local police units, customs offices, etc. are connected to SIENA. It has thus created a web linking not just EU member states but also some third parties Europol has cooperation agreements with countries like Switzerland, as indicated in the Swiss report, and they too use SIENA for information exchange.[36] SIENA is considered the mandatory channel for many forms of cooperation under evolving EU law for example, a recent directive on law enforcement information exchange proposes that by default, cross-border requests go through SIENA to ensure security and traceability. It's integrated with Europol's other systems: if a message concerns data that should go into the Europol Information System EIS Europol's central database of criminal targets and cases, analysts can do so. Conversely, a hit in the EIS can trigger a SIENA message to follow up with the country that owns the data. SIENA, therefore, acts as both a proactive and reactive tool in interoperability. Effectiveness: SIENA's use has grown exponentially as trust in the system grew and law enforcement realized the necessity of rapid information sharing. [37]In 2023, SIENA handled about 1.79 million messages among participants, reflecting an 11% increase from the previous year. By 2024, it crossed 2 million messages annually. [38]These messages cover a wide gamut drug trafficking intelligence, counter-terrorism info, cybercrime leads, human trafficking cases, financial crime intelligence, etc. One of SIENA's strengths is supporting joint investigations: when multiple countries form a Joint Investigation Team JIT to tackle a criminal group, SIENA becomes the daily conduit for sharing operational

[35] Europol, *Agreement with Europol* https://www.europa.eda.admin.ch/en/agreement-europol accessed 25 May 2026.

[36] Europol, *More than 3,000 Law Enforcement Authorities Now Connected to Europol* (Press Release, 2023) https://www.europol.europa.eu/media-press/newsroom/news/more-3-000-law-enforcement-authorities-now-connected-to-europol accessed 25 May 2026.

[37] Europol, *More Than 3,000 Law Enforcement Authorities Now Connected to Europol*https://www.europol.europa.eu/media-press/newsroom/news/more-3-000-law-enforcement-authorities-now-connected-to-europol accessed 25 May 2026.

[38] Europol, *Secure Information Exchange Network Application (SIENA)* https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena accessed 25 May 2026.

updates and intelligence within the team. The impact of SIENA can be illustrated by efficiency: what once took days or weeks via letters and diplomatic cables now happens in near real-time. This speed is crucial for pursuing criminals who can move across borders quickly. Europol has credited SIENA for many successes, such as coordinated raids in multiple countries where intelligence was shared ahead via SIENA messages to synchronize actions. It also contributes to information-led policing at the international level patterns detected in one country can be quickly disseminated to all to beware of similar modus operandi for example, a new credit card fraud scheme spotted in one nation can be alerted to others. One challenge with SIENA was ensuring all relevant agencies in member states were connected initially, communication might only have been between central units. But now, with thousands of agencies on board, a local police unit can be directly addressed if needed. Another challenge is maintaining security and confidentiality: Europol uses state-of-the-art encryption, and SIENA messages are considered highly secure to the point that some countries use SIENA to even transmit sensitive data in legal processes. The system's governance allows for multi-country communication while respecting national laws e.g., a country might mark certain intel as not to be used in court just intelligence, and SIENA infrastructure supports these handling caveats. Comparatively, SIENA differs from CCTNS/NCIC/PND in that it's not a database you can search to instantly retrieve records; it's a platform to ask others for information. Europol does have a separate database EIS, but SIENA is the communication tool. Interestingly, India's Interpol liaison CBI is Interpol's National Central Bureau in India uses a messaging system I-24/7 of Interpol somewhat analogous to SIENA, but at a global scale, albeit volumes are smaller and not as deeply integrated. The concept behind SIENA underscores that technology can overcome jurisdictional barriers if properly managed something India might consider in South Asian regional cooperation or between different law enforcement bodies CCTNS could perhaps have a secure communication add-on for inter-state coordination beyond database lookups, which currently often still rely on phone/email.[39][40]

Comparative Analysis

NCIC and PND represent two models. NCIC is centrally managed by a federal authority FBI with strict, uniform standards; data resides in one system accessible by all. PND, while centrally hosted, aggregates from many sources and thus has to accommodate diversity in input, reflecting a looser federation. CCTNS lies somewhere in between, it had a centralized design CAS software uniformity but deployed in a federated manner with state-owned databases. The hybrid model of CCTNS allowed more local control than NCIC states run their part of system, but also required greater effort to ensure consistency some states initially modified fields causing incompatibility until standardization was enforced. The NCIC experience suggests that strong central oversight can ensure uniform quality, but India's federal structure necessitated a degree of decentralization.

All systems aim to provide comprehensive data for law enforcement, but their scope differs. NCIC focuses on critical identifiers stolen/wanted/missing, essentially a pointer system with relatively concise records. PND and CCTNS store richer narratives and intelligence case details, investigation info. This means CCTNS and PND face bigger data quality challenges free text, detailed reports are harder to standardize. NCIC's controlled data fields are easier to maintain and update e.g., a stolen vehicle entry is quite structured. As a result, NCIC can boast high accuracy though not perfect e.g., once a warrant is served, the record should be promptly removed to avoid false arrests. PND's weakness, per analyses, was inconsistency between forces in how diligently they uploaded data or how current it was. CCTNS tackled this by making real-time entry the norm police station is the point of origin, thereby ensuring data is up-to-date by design. A related aspect is volume: CCTNS, by digitizing all FIRs, etc., has a very large dataset 280 million records by 2021 just in national database, which dwarfs NCIC's 12 million active

[39] Europol, *Secure Information Exchange Network Application (SIENA)* https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena accessed 25 May 2026.

[40] Europol's Data Dominance: The Multifaceted Involvement and Impact of Data Analytics Across Sectors' *European Papers* https://www.europeanpapers.eu/e-journal/europol-data-dominance-multifaceted-involvement-impact-data-analytics-across-sectors accessed 25 May 2026.

records. But NCIC's figure is low because it's selective active wanted files etc., whereas CCTNS is comprehensive all cases, including those not currently active. This comprehensive approach serves broader purposes analytics, full case management but poses scalability and retrieval speed challenges. NCIC's narrow but deep approach versus CCTNS's broad approach shows different philosophies: one as a quick-check tool, the other as an all-in-one system.

All systems enhance interoperability, but at different levels. CCTNS and PND break silos within a country; NCIC and SIENA operate across jurisdictions states in US, nations in EU. Interoperability is not just technical but also organizational. NCIC succeeded by creating a "shared management concept"states are part of its governance. Europol's SIENA similarly works because countries collectively decide to use it as the standard channel. CCTNS, in early days, had to foster a collaborative mindset among statesNCRB formed committees with state representatives to agree on data sharing norms, similar to NCIC's advisory board practice. SIENA demonstrates that even without a supra-national police, information can flow if a trusted central intermediary Europol exists with secure technology. India's ICJS is analogous in trying to connect independent pillars police, courts, etc. who have different masters. The success of ICJS will depend on a strong central coordinating body NCRB and the e-Committee in this case and clear protocols, much like Europol's role for SIENA.

NCIC is highly effective because its use is deeply ingrained and it delivers immediate value to the officer on the street the 90-second stolen car hit story from 1967 or today's 0.1 second checks. CCTNS, to maximize effectiveness, similarly must be user-friendly and fast; the recent upgrades focusing on faster search and better UI tie into this. PND taught that simply having a system doesn't guarantee usage, it required mandates and showcasing results to become routine. The 2022 study showed some forces still not using all their PND licenses fully. CCTNS has seen a similar phenomenon where some features like analytics were underused, prompting renewed training. Another measure of effectiveness is how these systems have adapted to new crime types. NCIC, for instance, added files for terrorism and gangs as new threats emerged. CCTNS has been adding modules like cybercrime tracking, social media monitoring, etc., to stay relevant. PND is now used even for things like facial recognition searches which were not foreseen initially.

Privacy Framework Comparison

With great data comes great responsibility. Europe's SIENA operates in a strict privacy regime Europol is monitored by data protection authorities, and usage of SIENA info in court is carefully regulated via "handling codes" and legal agreements. The UK's PND has extensive guidance on proportional use, data accuracy and deletion, etc., rooted in UK data protection law. NCIC, while focused on police use, is governed by federal regulations 28 CFR Part 20 that ensure data is used for criminal justice purposes and individuals can challenge their records for accuracy. India's CCTNS emerged in a context without a dedicated data protection law until 2023. Now with the Digital Personal Data Protection Act, similar focus is shifting to ensure safeguards. Privacy concerns, such as potential surveillance or misuse of data, have been raised e.g., NGOs questioning if CCTNS data could be misused for profiling. Learning from the West, India is likely to strengthen oversight, possibly establishing independent audit mechanisms for CCTNS usage or giving citizens some recourse if data is wrong as one can in the US to correct NCIC/III records. Thus, in comparative terms, integrating a strong privacy regime is an area where CCTNS is catching up.[41]

Innovation and Future Outlook: Each system continues to evolve. NCIC's next gen aims to incorporate modern tech and user input; PND is slated to merge into a new platform LEDS with PNC; SIENA might get interconnected with other networks like FIU.net for financial intel units to broaden its reach. CCTNS as CCTNS 2.0 is integrating AI/ML: plans for predictive policing, NLP for analyzing FIR text, facial recognition, etc., are on the horizon. The ET Government article by Mohit Garg envisions possibilities like blockchain for evidence management and IoT

[41] Common Cause, *Status of Policing in India Report 2023*https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf accessed 25 May 2026.

integration for smart policing ideas that are also echoed in advanced policing discussions worldwide. This suggests a convergent evolution: all systems are looking to harness emerging tech to further enhance crime fighting predictive analytics, cross-database linkages, etc..

One notable difference is that NCIC and PND primarily serve law enforcement objectives, whereas CCTNS also doubles as an e-governance service platform for the public. In the US/UK, separate systems or processes handle citizen interaction like calling 911 or reporting online in some local system, but not NCIC directly. India has leveraged CCTNS to be both an investigative tool and a citizen service portal. This dual use is ambitious and offers convenience, but also means the system design had to consider user-friendliness for public access, which NCIC/PND did not. Overall, in comparative perspective, CCTNS holds up well for a country of India's size and complexity. It achieved in roughly a decade what NCIC took many more years to grow into at least in terms of connecting the whole nation. The lessons from abroad underline the importance of sustained training, policy support, and adaptability of these systems to changing needs. As policing challenges become increasingly transnational cybercrimes, terrorism, CCTNS might also eventually need to interface externally possibly connecting with Interpol databases or even one day exchanging with systems like PND or others under bilateral agreements, as crime has no borders. The foundational work of CCTNS puts India in a position to be a robust contributor to global criminal information exchange in the future.

CCTNS has successfully established a nationwide digital policing infrastructure, linking all police stations and key offices under a common platform. As of the mid-2020s, CCTNS coverage is virtually 100%, a significant achievement in a country with over 15,000 police stations. This has effectively eliminated information silos at the state and district levels, enabling quicker dissemination and retrieval of crime data across India.

The technical architecture of CCTNS balances central standardization with state-level autonomy. By deploying a Core Application Software uniformly but allowing state-specific extensions, CCTNS ensured data consistency needed for inter-state exchange. This architecture, complemented by the use of a national cloud infrastructure MeghRaj for hosting central systems, provides a scalable foundation. However, it also means that continuous coordination and version control are required as different states update or customize their systems, highlighting the need for strong governance a role NCRB is playing.

Implementation of CCTNS faced and overcame major challenges through adaptive strategies. Issues of connectivity were addressed by leveraging multiple technologies SWAN, BSNL, VSAT, BharatNet, though network reliability still needs improvement in some regions. Data migration from legacy systems was a pain point, but phased digitization and quality checks are gradually standardizing historical data. Human factors training and resistance were tackled by large-scale capacity building and by demonstrating the system's benefits e.g., success stories where CCTNS solved cases. Consequently, the project timeline extended beyond initial estimates, reaching substantial completion by around 2020 instead of 2012, but the extended timeline allowed for more comprehensive coverage and refinement.

CCTNS has notably improved policing effectiveness and inter-agency collaboration. The ability to perform national searches in seconds has enhanced investigative capabilities, leading to more timely arrests and property recoveries that would have been unlikely before e.g., suspects wanted in one state being caught in another. Integration via ICJS has begun to break down traditional walls between police, courts, prisons, and forensics, enabling a more holistic criminal justice process such as courts accessing FIRs electronically, or police knowing the custody status of an accused without delay. These improvements contribute to faster investigations and potentially faster trials, addressing a long-standing issue of delays in the justice system.

Citizen-facing services and transparency have improved under CCTNS. The project's citizen portals mean many members of the public can now interact with the police online, whether to file a report or obtain a verification, thus increasing convenience and transparency in police processes. Digital records reduce the scope for discretionary abuse an entry, once made, is auditable and cannot be easily manipulated or hidden, thereby strengthening accountability. There is also more data-driven oversight; senior officers use CCTNS dashboards to monitor station performance like number of FIRs, pendency of investigations, which was difficult with paper records.

Comparison with international systems shows CCTNS is conceptually on par, though contextually distinct. Like NCIC, CCTNS provides nationwide reach; like PND, it consolidates distributed data for unified search; akin to SIENA's aim, it fosters cross-jurisdiction cooperation. However, differences are notable:

NCIC's narrower focus mostly wanted and stolen indices means it is extremely fast and widely used at the tactical level, whereas CCTNS's broader data complete case info offers depth but with the challenge of extracting quick insights, something being mitigated by improved search tools and planned AI integration.

PND's experience underscores the importance of uniform data entry and enthusiastic adoption. CCTNS, by virtue of being the primary system for police work not an optional intel sharing platform, likely enjoys better adoption in daily use than PND did initially. Still, the lesson remains that continuous training and demonstration of value are needed to ensure advanced features like analytics are fully utilized by officers, not just the basic FIR filing.

SIENA highlights the critical nature of secure and structured information exchange. While India does not have an exact parallel, CCTNS combined with ICJS is moving toward a similar integrated information exchange domestically. The idea of "one data, one entry" and maximizing re-use that SIENA embodies in Europe is very much at the heart of CCTNS/ICJS in India. CCTNS has had a positive impact on crime data analytics and policy formulation at a macro level. With comprehensive data available, agencies like NCRB are now better equipped to analyze crime trends year over year, identify emerging crime hotspots, and advise policy changes. The data from CCTNS feeds into national statistics, enabling evidence-based policymaking for instance, if CCTNS data shows a rise in cybercrime nationwide, it justifies investment in cyber police stations and training.

Ensuring that all states maintain high data quality correct entries, regular updates, avoiding duplications is an ongoing effort. Automated validation, as proposed, and periodic data audits can help. Upgrading connectivity infrastructure perhaps moving toward 4G/5G backups, diversifying ISPs is needed to address the connectivity issues that still hamper usage in some remote areas. While basic computer literacy is no longer the barrier it once was, using data effectively like doing complex searches or using analytics tools requires higher skill levels. Continuous professional development and perhaps inducting specialized "crime analysts" at district levels could maximize CCTNS's potential. As India operationalizes data protection law, CCTNS must adapt to comply, for instance, defining clear data retention periods, procedures for individuals to seek correction of data, and robust protection against unauthorized access. Security measures like multi-factor authentication for users and AI-based monitoring for unusual access patterns, as suggested by experts, should be standard. There remain law enforcement entities not yet integrated into CCTNS e.g., the Narcotics Control Bureau, Enforcement Directorate, Railway Protection Force for FIRs in their jurisdiction, etc.. Plans exist to onboard such agencies into the network. This will further enrich the system, and efforts should continue in this direction for truly comprehensive coverage of all criminal cases, irrespective of investigating agency. With CCTNS, India has built a platform that potentially could interface internationally. For example, interoperability with Interpol systems automating lookup of Interpol notices through CCTNS could be explored. In comparison to systems abroad, CCTNS positions India among the leading countries in terms of a unified criminal information system. Many countries still operate fragmented systems; India's experience might serve as a model for other federated nations trying to integrate criminal data. Conversely, India can glean from NCIC's decades of continuous improvement and Europol's robust data governance practices to refine CCTNS further.

CCTNS has had a transformative impact on Indian policing by ushering in an era of digital record-keeping and interconnectivity. Its implementation journey, though prolonged and challenging, has largely delivered the intended outcomes of improved police efficiency, better crime tracking, enhanced collaboration, and improved citizen services. The comparative analysis reaffirms that while technological systems must be tailored to local contexts, the underlying principles of data sharing, standardization, and user engagement are universal. CCTNS's progress and impact thus far provide a strong foundation for future advancements in smart policing and integrated criminal justice delivery in India.

Conclusion

The Crime and Criminal Tracking Network and Systems CCTNS project stands as a landmark in the modernization of India's criminal justice information infrastructure. This research paper examined CCTNS from multiple angles, its technical design, the challenges and achievements in its implementation, its measurable and perceived impacts on policing and public service, and how it compares with prominent international systems like the US NCIC, UK PND, and Europol's SIENA. Through this comprehensive analysis, several conclusions can be drawn. First, CCTNS has fundamentally re-engineered information management in Indian policing. It has transitioned police operations from a paper-bound, localized model to a digitally integrated, national model. Information that once took weeks to circulate now flows almost instantly to those who need it. This has enhanced the responsiveness of law enforcement and provided frontline officers with better tools to do their jobs. In doing so, CCTNS has validated the vision that guided its creation that leveraging information technology in policing can lead to significant gains in efficiency, effectiveness, and accountability. The project's completion of connecting all police stations and digitizing records is an accomplishment on the scale of India's vast bureaucracy that should not be understated.[42] Second, the success of CCTNS, tempered by lessons learned, offers insights for similar large-scale e-governance initiatives. Key among these lessons is the importance of stakeholder buy-in and capacity building: technology is only as good as its users. Early hurdles faced by CCTNS in training personnel highlight that major investments in continuous training and change management are as essential as investments in hardware and software. Additionally, CCTNS demonstrated the need for adaptability the project's timeline extensions and scope enhancements CCTNS 2.0 features show that flexibility in planning is crucial when breaking new ground. The phased approach, pilot testing, and iterative rollout helped in risk mitigation and course correction when needed for instance, addressing network issues or software bugs identified in pilots before scaling up. Third, integration is the new frontier that CCTNS has enabled but not fully realized yet. With CCTNS providing the base, India is now poised to achieve true criminal justice integration through ICJS, linking courts, prisons, forensics, prosecution and police in one data-sharing ecosystem. This aligns with global trends where siloed information systems are giving way to interconnected platforms to improve the justice process holistically. The groundwork laid by CCTNS common data standards, a central querying capability, and collaborative institutional structures will serve as a backbone for these integrations. The coming years, with ICJS Phase II underway, will likely see even greater dividends in terms of speedy trials, improved conviction rates, and smarter policing fueled by comprehensive data. Comparatively, the study finds that CCTNS is a peer to international systems and in some aspects more ambitious. Unlike NCIC or PND, which focus on either critical shared data or aggregated intelligence, CCTNS attempts both: it is an investigative workflow system and a national search database and a public service portal all in one. This comprehensive scope is bold and has required balancing different objectives internal efficiency vs. public accessibility, for example. While this breadth adds complexity, it also yields synergies a digital FIR benefits the investigator, the citizen in tracking its status, and the court for access simultaneously, embodying a whole-of-system improvement. That said, the comparison also highlights areas for improvement: for example, NCIC's stringent data quality regime and UK's code of practice for using shared data responsibly could inform enhancements in CCTNS's governance and standard operating procedures.[43] Europol's experience underscores the importance of secure data exchange and respecting privacy, a call that CCTNS must heed as data volumes and sensitivity grow. In terms of effectiveness, the ultimate measure of CCTNS's success will be reflected in metrics like crime detection rates, response times, and public trust in policing.[44] While it is hard to isolate CCTNS's contribution to these outcomes quantitatively since many factors influence crime and policing, anecdotal evidence and user testimonies strongly suggest a positive influence. Faster information access has led to more crimes solved and possibly deterred some as criminals become aware that police databases are better connected. The public's ease of lodging complaints and accessing services may not directly reduce crime, but it does improve trust and satisfaction with the justice system, an important outcome in itself, aligning with the goal of SMART policing Sensitive, Modern, Accountable, Responsive, Tech-savvy.

[42] Ibid n.16
[43] Ibid n.28
[44] Ibid n. 36

Looking ahead, sustaining and advancing CCTNS will require ongoing commitment and innovation. Technology projects are not one-off endeavors; they need upgrades, maintenance, and adaptation to new requirements. Regular funding for maintenance for servers, networks, and cybersecurity, periodic training refreshers for personnel due to transfers and new inductions, and policy support to mandate and institutionalize the use of the system are essential. Moreover, as the paper discussed future opportunities AI analytics, IoT integration, mobile platforms for police, etc. leveraging these within CCTNS could propel Indian policing into a new era of predictive and preventive capabilities. For instance, integrating a crime analytics module that uses machine learning on CCTNS data to forecast hotspots could help deploy police proactively. The conclusion from international comparisons is clear: these systems are most effective when they don't stagnate. NCIC, PND, and SIENA are each in phases of significant upgrade or integration. CCTNS will similarly need a roadmap for the next 5-10 years indeed NCRB's agenda on linking NAFIS, AFRS, etc., is a step in that direction. In conclusion, CCTNS has been a game-changer for India's internal security apparatus, laying a digital foundation that enhances crime-fighting and service delivery. It illustrates how a well-conceived information system, despite implementation hurdles, can bring about transformative change in a vital sector of governance. The positive outcomes observed affirm the value of such e-governance initiatives and provide encouragement to pursue further innovations. As crime and criminals become more sophisticated and transnational, systems like CCTNS especially when networked with their peers globally will be indispensable in preserving law and order and delivering justice efficiently. The journey of CCTNS from 2009 to now is a testament to the power of information systems in governance, and it offers a blueprint for future projects aiming to harness technology for public good.

The Crime and Criminal Tracking Network and Systems CCTNS represents a transformative shift in India's criminal justice and policing landscape by establishing a digitally integrated framework for crime management, information exchange, and inter-agency coordination. Conceived initially as a technological intervention for modernising police administration, CCTNS has evolved into a foundational public digital infrastructure supporting data-driven policing, citizen services, and institutional interoperability across the criminal justice ecosystem. Its integration with allied platforms under the Inter-operable Criminal Justice System ICJS demonstrates the gradual transition from isolated digitisation efforts towards a unified justice information architecture.

However, this study demonstrates that the significance of CCTNS extends beyond technical architecture and operational efficiency. The scale, complexity, and continuing expansion of the system reveal important financial and governance dimensions that position CCTNS within the broader discourse of public digital infrastructure and business law. Large-scale investments in software development, connectivity infrastructure, cybersecurity, cloud integration, maintenance, vendor management, and capacity building require sustained financial planning and accountability mechanisms. Consequently, the long-term success of CCTNS depends not only upon technological deployment but equally upon effective procurement practices, lifecycle governance, contractual compliance, risk allocation, and fiscal sustainability. The transformation of CCTNS into an evolving digital ecosystem therefore necessitates stronger frameworks for public expenditure monitoring, audit mechanisms, data governance, and technology regulation.

The comparative analysis with international systems such as the United States' NCIC, the United Kingdom's PND, and Europol's SIENA further indicates that effective criminal information systems derive their value not merely from technological interoperability but from governance interoperability. Cross-border information exchange, mutual legal assistance frameworks, international policing cooperation, and evolving data protection obligations increasingly influence the operational environment of domestic policing databases. In this context, CCTNS must progressively align with internationally accepted standards relating to cybersecurity, privacy protection, auditability, and secure information-sharing mechanisms.[45][46][47]

[45] Ibid n.20
[46] Ibid n.32
[47] Ibid n. 35

Accordingly, the future trajectory of CCTNS lies in its evolution from a policing information network into a mature digital governance platform characterised by financial accountability, regulatory compliance, and international compatibility. As India advances towards integrated digital justice systems, CCTNS offers an important model demonstrating that technological modernisation in criminal justice must be accompanied by robust governance structures, sustainable financing mechanisms, and globally responsive institutional frameworks.

References

[1] Bain A and Sutton A, 'What Does the UK Police National Database Tell Us About the Future of Police Intelligence?' *Policing: A Journal of Policy and Practice*https://academic.oup.com/policing/article/doi/10.1093/police/paac074/6686660 accessed 25 May 2026.

[2] Common Cause and Lokniti-CSDS, *Status of Policing in India Report 2023: Surveillance andPrivacy* 2023 https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf accessed 25 May 2026.

[3] Common Cause, *Status of Policing in India Report 2023*https://www.commoncause.in/wotadmin/upload/REPORT_2023.pdf accessed 25 May 2026.

[4] Comptroller and Auditor General of India, *Information Systems Audit of Crime and Criminal Tracking Network and Systems CCTNS, Uttar Pradesh*, Report No 5 of 2018.

[5] Comptroller and Auditor General of India, *Report on Information Systems Audit of Crime and Criminal Tracking Network and Systems CCTNS* https://cag.gov.in/uploads/icisa_it_reports/7db9b967001ebeec572b498754f61af4.pdf accessed 25 May 2026.

[6] Dhalai District Police, Tripura, *Advantages of CCTNS* https://dhalaipolice.tripura.gov.in/intralink accessed 25 May 2026.

[7] e-Committee, Supreme Court of India, *Inter-Operable Criminal Justice System ICJS* https://ecommitteesci.gov.in/icjs/accessed 25 May 2026.

[8] *ETGovernment*, 'CCTNS 2.0 ICJS Meghraj Cloud: Revolutionizing India's Criminal Justice System with CCTNS 2.0 and ICJS Integration' https://government.economictimes.indiatimes.com/blog/revolutionizing-indias-criminal-justice-system-with-cctns-20-and-icjs-integration/123422358 accessed 25 May 2026.

[9] Europol, *Agreement with Europol* https://www.europa.eda.admin.ch/en/agreement-europol accessed 25 May 2026.

[10] Europol, *More than 3,000 Law Enforcement Authorities Now Connected to Europol* Press Release, 2023 https://www.europol.europa.eu/media-press/newsroom/news/more-3-000-law-enforcement-authorities-now-connected-to-europol accessed 25 May 2026.

[11] Europol, *More Than 3,000 Law Enforcement Authorities Now Connected to Europol*https://www.europol.europa.eu/media-press/newsroom/news/more-3-000-law-enforcement-authorities-now-connected-to-europol accessed 25 May 2026.

[12] Europol, *Secure Information Exchange Network Application SIENA* https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena accessed 25 May 2026.

[13] Europol, *Secure Information Exchange Network Application SIENA* https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena accessed 25 May 2026.

[14] Europol's Data Dominance: The Multifaceted Involvement and Impact of Data Analytics Across Sectors' *European Papers* https://www.europeanpapers.eu/e-journal/europol-data-dominance-multifaceted-involvement-impact-data-analytics-across-sectors accessed 25 May 2026.

[15] Evidence2e-CODEX, *SIENA Workshop Documentation* https://evidence2e-codex.eu/p/d/2/d2-01e2eworkshop20190327panel5-siena-431.pdf accessed 25 May 2026.

[16] Federal Bureau of Investigation, Criminal Justice Information Services Division, *NCIC Record: 5.6 Million Queries in a Single Day* 15 February 2006 https://archives.fbi.gov/archives/news/stories/2006/february/ncic021506 accessed 25 May 2026.

[17] Federal Bureau of Investigation, Criminal Justice Information Services Division, *NCIC Turns 50* 27 January 2017 https://www.fbi.gov/news/stories/ncic-turns-50 accessed 25 May 2026.

[18] Federal Bureau of Investigation, *NCIC Record: 5.6 Million Queries in a Single Day*https://archives.fbi.gov/archives/news/stories/2006/february/ncic021506 accessed 25 May 2026.

[19] Federal Bureau of Investigation, *NCIC Turns 50* https://www.fbi.gov/news/stories/ncic-turns-50 accessed 25 May 2026.

[20] Federal Bureau of Investigation, *The FBI's National Crime Information Centre*https://archives.fbi.gov/archives/news/testimony/the-fbis-national-crime-information-Centre accessed 25 May 2026.

[21] Federal Department of Foreign Affairs Switzerland, *EuropolSIENA Exchange with Switzerland* 27 January 2025 https://www.europa.eda.admin.ch/en/agreement-europol accessed 25 May 2026.

[22] Garg M, 'CCTNS 2.0 and ICJS Integration with Meghraj Cloud: Transforming India's Criminal Justice System' *ET Government* 21 August 2025 https://government.economictimes.indiatimes.com/blog/revolutionizing-indias-criminal-justice-system-with-cctns-20-and-icjs-integration/123422358 accessed 25 May 2026.

[23] Government of India, Ministry of Home Affairs, *Development of Tools for Mainstreaming Disaster Risk Reduction in Environment SectorCCTNS Report* https://www.mha.gov.in/sites/default/files/IIPA-Report-CCTNS.pdf accessed 25 May 2026.

[24] Government of India, Ministry of Home Affairs, *Digital PoliceAbout Us*https://digitalpolice.gov.in/DigitalPolice/AboutUs accessed 25 May 2026.

[25] Government of India, Ministry of Home Affairs, *Inter-Operable Criminal Justice System ICJS*https://www.mha.gov.in/en/commoncontent/inter-operable-criminal-justice-system-icjs accessed 25 May 2026.

[26] Government of India, Press Information Bureau, *Press Release* https://www.pib.gov.in/PressReleasePage.aspx?PRID=2039059 accessed 25 May 2026.

[27] Home Office UK, *Code of Practice on the Operation and Use of the Police National Database*https://assets.publishing.service.gov.uk/media/5a7b8841ed915d4147620fc5/9999102808.pdf accessed 25 May 2026.

[28] Home Office UK, *Police National Database 1.5 Transformation Accounting Officer Assessment 12 September 2024*https://www.gov.uk/government/publications/home-office-major-programmes-accounting-officer-assessments/12-september-2024-police-national-database-15-transformation-accounting-officer-assessment accessed 25 May 2026.

[29] Kirkpatrick MD, 'Testimony on the National Crime Information Centre NCIC' Statement before the United States Senate, 13 November 2003.

[30] KPMG India, 'Enhancing Efficiency and Effectiveness in Policing with the Crime and Criminal Tracking Network and Systems CCTNS' https://kpmg.com/in/en/insights/2024/11/kpmg-make-the-difference/case-study-enhancing-efficiency-and-effectiveness-in-policing-with-the-crime-and-criminal-tracking-network-systems-cctns.html accessed 25 May 2026.

[31] KPMG India, *Enhancing Efficiency and Effectiveness in Policing with Crime and Criminal Tracking Network and Systems CCTNS* 24 March 2025 https://kpmg.com/in/en/insights/2024/11/kpmg-make-the-difference/case-study-enhancing-efficiency-and-effectiveness-in-policing-with-the-crime-and-criminal-tracking-network-systems-cctns.htmlaccessed 25 May 2026.

[32] Ministry of Home Affairs, Government of India, *Inter-Operable Criminal Justice System ICJS Project* updated 13 September 2024 https://www.mha.gov.in/en/commoncontent/inter-operable-criminal-justice-system-icjs accessed 25 May 2026.

[33] National Crime Records Bureau, *Digital Police PortalAbout CCTNS* Ministry of Home Affairs, status as of 1 July 2021 https://digitalpolice.gov.in/DigitalPolice/AboutUs accessed 25 May 2026.

[34] National Crime Records Bureau, *Digital Police PortalAbout Us* 2017 https://digitalpolice.gov.in/DigitalPolice/AboutUs accessed 25 May 2026.

[35] North Yorkshire Police, *Police National Database Procedure* https://www.northyorkshire.police.uk/SysSiteAssets/foi-media/north-yorkshire-police/our-policies-and-procedures/criminal-justice/police-national-database-procedure3.pdfaccessed 25 May 2026.

[36] Phythian R and Kirby S, 'What Does the UK Police National Database Tell Us About the Future of Police Intelligence?' 2023 17 *Policing: A Journal of Policy and Practice*https://academic.oup.com/policing/article/doi/10.1093/police/paac074/6686660 accessed 25 May 2026.

[37] Press Information Bureau, Government of India, 'Phase-II of Inter-Operable Criminal Justice System ICJS' Written Reply in Lok Sabha, 30 July 2024 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2039059 accessed 25 May 2026.

[38] Puducherry Police, *CAS Functionality and Services* https://police.py.gov.in/CCTNS%20CAS%20-%20MHA.pdf accessed 25 May 2026.

[39] SlideShare, *CCTNS Presentation* https://www.slideshare.net/slideshow/cctns/19344258 accessed 25 May 2026.

[40] UK Home Office, *Code of Practice on the Operation and Use of the Police National Database* 2010 https://assets.publishing.service.gov.uk/media/5a7b8841ed915d4147620fc5/9999102808.pdf accessed 25 May 2026.