

Four Contemporary Technology Trends in the Criminal Justice System

Posted on November 9, 2024

Introduction

Technology now shapes how [criminal-justice](#) agencies observe events, collect evidence, write reports, identify people, allocate resources, communicate with courts, and disclose information to the public. The original report identifies dash cameras, body-worn cameras, artificial intelligence, and automated report writing as four important trends. Its claims need greater precision. Cameras do not automatically create accountability, predictive systems can reproduce the biases in historical data, and an AI-generated narrative cannot replace an officer's independent memory and legal responsibility. This report preserves the four-trend structure while examining implementation, evidentiary integrity, privacy, accuracy, disclosure, and the effect of new tools on professional report writing (National Institute of Justice; Hollywood et al., 2018; National Institute of Standards and Technology, 2023).

Trend One: In-Car and Body-Worn Video

Dash cameras and body-worn cameras create time-stamped audiovisual records of police encounters, traffic stops, pursuits, searches, arrests, and statements. Video can support evidence, training, complaint review, and supervision, but its perspective is limited by camera position, activation, lighting, sound, obstruction, and what occurred before recording began. A body camera does not see exactly what an officer or civilian saw, and viewers may give video more authority than it deserves. Effective use requires policies governing activation, notice, retention, access, redaction, supervisor review, and prohibited manipulation. Accountability depends on those rules and on independent investigation, not simply on purchasing hardware. Agencies should also publish how often cameras fail or are not activated, because missing footage can be as important as recorded footage (National Institute of Justice, "Research on Body-Worn Cameras and Law Enforcement"; Dolly et al., 2026).

How Video Changes Report Writing

Video allows an officer to verify sequence, quoted language, timing, location, and visible actions, potentially improving the specificity of reports. It can also distort memory if the writer reviews footage before recording an independent account and later confuses what was personally perceived with what appeared on camera. Agencies should define when initial notes are made, when video may be reviewed, and how the report identifies that review. A report should explain relevant context rather

than merely direct the reader to hours of footage. Officers must document gaps, camera failures, activation delays, and important events outside the frame. The written report and audiovisual record should complement rather than substitute for each other (National Institute of Justice, “Research on Body-Worn Cameras and Law Enforcement”; Dolly et al., 2026).

Trend Two: Digital Evidence and Cloud-Based Management

Modern cases can involve mobile phones, social-media records, surveillance systems, license-plate readers, vehicle data, email, location information, and files stored across cloud services. Digital-evidence management platforms help agencies ingest, index, search, share, retain, and disclose these materials. They can reduce lost media and duplicate storage, but they create cybersecurity and access-control risks. Evidence must remain traceable from collection through courtroom presentation. Systems should record hashes, timestamps, user actions, transfers, redactions, and export history. Vendor contracts must address data ownership, breach notification, interoperability, deletion, and what happens when an agency changes providers. Convenience cannot weaken chain-of-custody requirements. Retention categories should follow law and case need rather than one indefinite default applied to every file (National Institute of Justice, resources on [digital evidence](#); Hollywood et al., 2018).

Digital Forensics and Authentication

Digital evidence is not self-authenticating merely because it appears on a device. Investigators need methods for preserving original data, creating forensic copies, documenting acquisition tools, interpreting metadata, and distinguishing user actions from automated system activity. Screenshots can omit context, and file dates can change during transfer. Encrypted devices, remote deletion, proprietary formats, and rapidly changing operating systems complicate recovery. Reports should state what was collected, by whom, under what authority, with which tool and version, and what limitations affected interpretation. A qualified examiner should avoid claiming that a device user personally created every artifact. Technical findings need translation into language that courts and nontechnical readers can evaluate (National Institute of Justice, resources on digital evidence).

Trend Three: Artificial Intelligence and Analytics

Artificial intelligence is used or studied for image analysis, speech transcription, gunshot detection, document review, risk assessment, link analysis, and pattern detection. In 2026, National Institute of Justice-sponsored research also examined automated analysis of body-camera recordings for procedural-justice behaviors. These systems can process volumes that humans cannot review quickly, but output remains probabilistic and dependent on training data, labels, thresholds, and deployment

conditions. AI should support investigation rather than establish guilt. Agencies need validation for the specific population and task, documented error rates, human review, and procedures for contesting results. A model's proprietary status does not eliminate due-process or disclosure obligations (Dolly et al., 2026; National Institute of Standards and Technology, 2023; Hollywood et al., 2018).

Facial Recognition and Biometric Search

Facial-recognition systems compare a probe image with one or many stored images and return possible matches according to a threshold. NIST's ongoing Face Recognition Technology Evaluation demonstrates that performance varies across algorithms, image quality, and use cases. A candidate list is an investigative lead, not a positive identification. Human reviewers can introduce confirmation bias, especially when they know the suspected person. Policies should require trained examiners, documented image preparation, meaningful corroboration, audit logs, and restrictions on low-quality or inappropriate images. Agencies must also consider demographic performance differences, retention of innocent people's images, surveillance at public events, and the legal authority for each database search (National Institute of Standards and Technology, *Face Recognition Technology Evaluation*).

Predictive Policing and Risk Assessment

Predictive systems attempt to estimate where crime may occur, who may be involved, or how likely a person is to reoffend or miss court. Historical data reflect enforcement choices as well as underlying conduct. If police repeatedly patrol one neighborhood, more incidents are recorded there, and the system may recommend still more patrol, creating a feedback loop. Risk scores can also conceal value judgments about which errors matter and which variables act as proxies for race or poverty. Agencies should test calibration, disparate impact, data quality, and practical benefit against simpler alternatives. High-stakes decisions require reasons that affected people and courts can understand and challenge (National Institute of Standards and Technology, 2023; Hollywood et al., 2018).

Trend Four: Automated and Generative Report Tools

Speech-to-text, form automation, computer-aided dispatch integration, and generative language systems can reduce repetitive data entry and help organize reports. A tool may import names, times, locations, call notes, or evidence identifiers, then propose a narrative. The danger is that plausible language can include invented details, omit uncertainty, merge different speakers, or reproduce errors from source systems. Officers remain responsible for every statement they sign. Agencies should prohibit fabricated content, require review against notes and evidence, preserve the prompts and generated versions where relevant, and mark machine assistance transparently. Automation

should increase accuracy and time for investigation rather than produce longer reports that appear polished but are less reliable (National Institute of Standards and Technology, 2023; National Institute of Justice, resources on artificial intelligence).

Translation and Accessibility Technologies

Automated translation, captioning, and transcription can improve access for witnesses, victims, attorneys, and court personnel, especially during initial triage. They are not universally adequate for legal consent, interrogation, or nuanced testimony. Dialect, background noise, code-switching, technical vocabulary, and trauma can produce serious errors. A report should distinguish machine translation from interpretation by a qualified human and should preserve the source audio or text. Accessibility also includes screen-reader-compatible reports, captions for video, and usable public-record portals. Technology can broaden participation, but only when agencies budget for verification and do not treat people with limited English proficiency or disabilities as acceptable sources of uncorrected data (National Institute of Standards and Technology, 2023).

Cybersecurity and System Resilience

A connected criminal-justice system becomes vulnerable to ransomware, credential theft, insider misuse, supply-chain compromise, and service outages. An attack can expose victims, confidential informants, sealed records, biometric data, or investigative methods. It can also interrupt dispatch, jail operations, evidence access, and court scheduling. Agencies need multifactor authentication, least-privilege access, encryption, backups, patch management, logging, vendor assessment, incident response, and continuity plans that work without the primary system. Report-writing systems should prevent unauthorized alteration and preserve earlier versions. Cybersecurity is part of evidentiary reliability and public safety, not merely an information-technology responsibility delegated away from leadership. Regular exercises should test whether staff can preserve evidence and continue lawful operations when networks are unavailable (National Institute of Standards and Technology, 2023).

Privacy and Data Minimization

Cameras, sensors, and analytical tools can collect information about people who are not suspected of wrongdoing. Bystanders, children, medical patients, protesters, and residents near monitored locations may enter databases through routine contact. Data minimization asks whether information is necessary, how long it should be retained, who may access it, and whether secondary use is justified. Unlimited storage can seem attractive for future investigation, but it increases breach and surveillance risk. Policies should distinguish evidentiary material from non-evidentiary recording, establish deletion schedules, protect sensitive locations, and document exceptional access. Public notice and independent oversight help communities evaluate whether benefits justify the scope of

collection (National Institute of Standards and Technology, 2023; National Institute of Justice, “Research on Body-Worn Cameras and Law Enforcement”).

Bias, Validation, and Human Oversight

Human oversight is meaningful only when reviewers have authority, time, and information to reject an automated recommendation. A person who routinely approves a system’s output without understanding its limitations does not provide a genuine safeguard. Validation should occur before deployment and continue after software, data, or operational context changes. Agencies should monitor false positives, false negatives, demographic disparities, overrides, complaints, and downstream outcomes. Procurement claims from vendors are not independent evidence. Pilot studies, external evaluation, transparent policies, and sunset clauses can prevent an experimental tool from becoming permanent through habit. Bias is not solved by removing human judgment; it must be examined in both human and technical processes (National Institute of Standards and Technology, 2023).

Discovery, Courtroom Use, and Explainability

Technology changes what prosecutors must disclose and what defense counsel may need to test. Relevant materials can include source data, audit logs, software versions, validation studies, thresholds, analyst notes, and machine-generated intermediate results. Courts may need expert testimony to understand limitations without allowing technical complexity to overwhelm the fact-finding process. Agencies should plan for disclosure when procuring a system rather than discover later that a vendor claims trade secrecy. Explainability does not always require publishing source code, but the parties need enough information to evaluate how evidence was produced, whether errors are known, and whether the method was applied correctly in the individual case (National Institute of Standards and Technology, 2023; Hollywood et al., 2018).

Training and Professional Judgment

New equipment does not reduce the need for writing, observation, interviewing, ethics, and legal knowledge. Officers and analysts must learn what a system measures, what it does not measure, and how to document reliance on it. Supervisors need training to identify copied narratives, unsupported certainty, and technology-driven shortcuts. Prosecutors and defense lawyers need enough technical literacy to ask informed questions, while judges and jurors need clear explanations. Training should use realistic failure scenarios, not only successful demonstrations. Professional judgment is strongest when users can articulate why they accepted or rejected an output and can continue essential work during system failure (Hollywood et al., 2018; National Institute of Standards and Technology, 2023).

Future of Criminal-Justice Reporting

Future reports will likely integrate structured data, video references, sensor records, automated transcription, and machine-assisted timelines. That integration can make evidence easier to navigate, but it may also encourage a false belief that a complete digital record exists. Important context remains unrecorded, and systems reflect decisions about what to capture. The best future report will be concise, traceable, and explicit about source and uncertainty. It will distinguish direct observation, witness statement, database result, inference, and automated suggestion. Agencies should evaluate technology according to accuracy, fairness, security, workload, and legitimacy rather than novelty. A tool is successful only when it improves justice, not merely when it accelerates processing (Hollywood et al., 2018; National Institute of Standards and Technology, 2023).

Conclusion

Four contemporary trends—police video, digital-evidence management, artificial intelligence and biometrics, and automated report generation—are transforming criminal-justice communication. They can preserve evidence, organize large records, identify patterns, and reduce repetitive work. They can also magnify surveillance, bias, cybersecurity risk, evidentiary opacity, and unverified narrative. Cameras require policy and context; digital evidence requires authentication and chain of custody; AI requires validation and contestability; automated writing requires human verification and preserved source material. The future of reporting should not be defined by replacing professional judgment. It should use technology to make each factual claim more traceable, each limitation more visible, and each high-stakes decision more accountable (National Institute of Justice; National Institute of Standards and Technology, 2023; Hollywood et al., 2018).

References

1. National Institute of Justice. "Research on Body-Worn Cameras and Law Enforcement."
2. Dolly, Colby, et al. *Multi-Modal Analysis of Body-Worn Camera Recordings*. National Institute of Justice, 2026.
3. National Institute of Standards and Technology. *Face Recognition Technology Evaluation*. Ongoing program.
4. National Institute of Standards and Technology. *Artificial Intelligence Risk Management Framework*. 2023.
5. Hollywood, John S., et al. *Addressing Emerging Trends to Support the Future of Criminal Justice*. RAND Corporation, 2018.
6. National Institute of Justice. Resources on digital evidence, artificial intelligence, and equipment technology.