Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.132:004.8

Article's History:
Received: 23.06.2025; Revised: 10.11.2025; Accepted: 16.12.2025

The implementation of artificial intelligence in Singapore's legal practice: Potential and risks for criminal investigations

Raimundas Jurka*
Doctor of Philosophy, Professor
Mykolo Romerio University
LT-08303, 20 Ateities Str., Vilnius, Lithuania
https://orcid.org/0000-0002-9911-5611

Abstract. The aim of this study was to assess the conditions for applying algorithmic systems in the activities of law enforcement and judicial oversight bodies in Singapore, in order to determine the boundaries of their admissibility with regard to the guarantees of due process. The methodology was based on normative-analytical, risk-oriented, structural-logical modelling, analytical synthesis, and case-study methods. It has been established that Artificial Intelligence automates cognitive tasks (classification, prediction); however, the results of machine learning are probabilistic and require regular quality testing and monitoring. In practice, AI analytics primarily generate "candidate" signals (anomalies, risk rankings) that require independent confirmation. The evidentiary status of digital traces arises after the provenance is recorded, and the integrity and verifiability of the materials are ensured. In financial crimes, technologies scale up both investigations and prevention, but automation creates a "risk paradox": errors in data or settings scale as rapidly as the positive effects of the system. It was found that Singapore's courts permit the use of Generative Artificial Intelligence only as an ancillary tool, placing full responsibility on the user for the accuracy and correctness of the submitted materials. The use of the Scam Analysis and Tactical Intervention System Plus enabled the triage of 7,200 monikers and the issuance of 3,700 directions under the Online Criminal Harms Act. Concurrently, the implementation of the Automation of Scam-fighting Tactics & Reaching Out ensured the automation of SMS alert dissemination, which helped prevent losses amounting to $420.41 million. At the same time, judicial practice indicates that operational effectiveness is not synonymous with evidentiary admissibility, as the authenticity of data requires a separate justification of the algorithmic output's reliability. To minimise procedural risks, it is advisable to apply standardised mechanisms for logging, model version control, error documentation, and independent verification. The practical significance lies in the application of the results by law enforcement agencies, prosecutors, courts, and the defence in Singapore when evaluating and using algorithmic results in criminal proceedings

Keywords: reliability; algorithm; reproducibility; data; verification; triage

Introduction

Artificial Intelligence (AI) is used in criminal law enforcement as a tool for processing digital data, identifying patterns in large volumes of information, supporting cybercrime investigations, and applying biometric identification. In Singapore, such applications are developing against a backdrop of high public sector digitalisation and the establishment of national approaches to AI governance, which intensifies the requirements for procedural safeguards in criminal proceedings. In this context, the central issue is the legal-procedural admissibility of AI decisions: the ability to ensure the verifiability and reproducibility of results, the possibility of independent review and appeal, as well as compliance with the principles of proportionality and non-discrimination in cases where potential errors can affect the scope of an individual's rights and freedoms.

Suggest Citation:
Jurka, R. (2025). The implementation of artificial intelligence in Singapore's legal practice: Potential and risks for criminal investigations. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 62-74.

*Corresponding author

The academic literature presents a heterogeneous body of knowledge concerning these challenges in the Singaporean context. In the work of J.G. Allen *et al.* (2025), Singapore's AI governance is conceptualised as a multi-level regulatory architecture combining guiding principles, institutional mechanisms, and tools to enhance trust in AI. This helped outline criteria for assessing the legitimacy of AI applications in criminal justice, particularly the relevance of accountability, standardisation, and control for law enforcement practices where the consequences of errors carry heightened procedural significance. The research by N.F.-Z. Lim & K.S. Tan (2025) systematised the legal environment for AI regulation in Singapore and demonstrated how risk-oriented approaches are combined with pro-innovation policies. This enabled the formulation of criteria by which legal requirements for AI decisions should be strengthened in high-risk domains (criminal investigations and evidence analysis), serving as a normative basis for justifying the boundaries of permissible AI use and control requirements. S.S. Lim & G. Chng (2024) examined Singaporean AI-assurance practice through the lens of verification tools and substantiated its role in ensuring the transparency and manageability of AI systems. The formalisation of checks and standardised assessment procedures can reduce technical uncertainty and increase trust in system outputs. This provided grounds to link technical "verifiability" with procedural requirements for evidentiary information and to justify the need for independent evaluation of AI-generated conclusions in criminal cases.

The evidentiary issues are addressed in the work of D. Seng & S. Mason (2021), which examined the implications of using AI for generating evidentiary information and assessing its reliability. The authors showed that for "machine" conclusions, the ability to provide an explanation, access to data on the system's functioning, and procedural controllability of error risks are critical. This laid the foundation for countering the manipulation of digital materials, which has direct significance for modern 21st-century forensic science. The socio-legal consequences of technological surveillance were documented by G. Beltrão *et al.* (2025). The authors investigated the conditions of trust in facial recognition systems within the context of mass surveillance, demonstrating the dependence of such systems' acceptability on perceptions of legitimacy and social justifiability. This suggests that the application of biometric tools for identification and suspect location must consider public trust as a factor influencing the legitimacy of the relevant practices. Using the digital tool TraceTogether as a case study, research by T. Lee & H. Lee (2020) and H. Lee & T. Lee (2022) analysed the mechanisms of normalising surveillance and rationalising data use in public administration. Although these studies are not exclusively focused on AI, they demonstrate how digital infrastructures create conditions for the cross-sectoral transfer of data into law enforcement practices. This indicates that technological solutions can alter the balance between efficiency and privacy guarantees.

The work of A.A. Khan (2024) examined Singaporean approaches to combating cybercrime, emphasising the growing role of digital traces and analytical tools in policing. The author's conclusions are relevant for understanding the operational needs and limitations of investigations, as well as for posing the question of the conditions under which analytical findings can be integrated into procedural decisions without lowering standards of justification. In a study by J. Chase *et al.* (2021), it was established that the GRAND-VISION system can generate operationally viable daily patrol deployment plans based on predicting spatio-temporal demand, considering personnel and time constraints. This demonstration of a real-world AI application scenario within the Singapore Police outlined legal risks for criminal law enforcement (dependency of decisions on the quality of historical data and the potential reproduction of previous patrolling practices), necessitating accountability and proportionality control. The comparative perspective in the work of H. Alibašić (2025) allowed for an observation of how Singapore's AI policy relates to other jurisdictions and international influences. This provides a basis for determining which elements of governance are context-dependent and which can be transferred in the form of general standards.

The existing body of scientific literature describes AI governance, issues of trust, and the risks of surveillance. However, there is a lack of systematic comparison of these aspects with the requirements of criminal procedure concerning evidence and procedural fairness, particularly in Singapore. Therefore, the aim of this study was to assess the use of artificial intelligence in criminal investigations in Singapore, specifically in evidence analysis. To achieve this aim, the following tasks were set: to systematise the areas of AI application relevant to criminal investigations, to identify risks and potential benefits based on real-world cases of digital technology application by law enforcement in Singapore, and to formulate criteria for the responsible use of AI systems.

Materials and Methods

This study integrated normative-analytical and risk-oriented approaches, structural-logical modelling, analytical synthesis, and case-study methods, applied to the analysis of electronic and algorithmically generated data in the criminal process of Singapore. The Singaporean context was utilised as an illustrative example of the balance between technological innovation and procedural safeguards, thereby ensuring the practical orientation of the research. This approach enabled the identification of key control vectors and the translation of ethical principles into formalised parameters to ensure the contestability of outcomes in court. The normative-analytical analysis method was employed to examine approaches to regulating AI and Generative AI (GenAI) within Singapore's legal framework across the following dimensions: evidentiary admissibility, algorithmic transparency, and personal data protection. The analysis was conducted based on the framework document

(guidelines) issued by the Personal Data Protection Commission (2020) of Singapore, the proposed framework by the AI Verify Foundation (2024), and a press release from the Infocomm Media Development Authority (2024). The selection of sources was determined by their complementarity: they simultaneously provide a regulatory framework for the responsible use of AI, a diagnostic assessment of the risks of "hallucinations", and global standards for AI assurance.

The structural-logical modelling method was used to develop and describe the architecture of a criminal justice ecosystem that links technological data processing with the procedural outcome: data → processing → forensics, through the chain "→ procedural verification". Two fundamental operational modes of the systems were described: the alert-triage mode for identifying suspicious objects and the operational-intervention mode for scaled response. This allowed for a distinction to be made between the technical authenticity of a digital record and the reliability of its algorithmic interpretation, yielding a quantitatively interpretable result regarding operational efficiency and evidentiary admissibility. Through analytical synthesis, managerial controls (logging, version control, "human-in-the-loop" verification) were systematically and methodically linked with indicators of procedural reliability to formulate an applied implementation framework. The Evidence Act of the Republic of Singapore (1997) and the judicial guideline Guide on the Use… (2024) were utilised. Furthermore, the report from the Singapore Courts (2024) and the official description of the technical capabilities of the government agency, the Home Team Science and Technology Agency (HTX) (2025), were analysed. The selection of these resources was justified by their capacity to provide comparable indicators of transparency and the investment-project feasibility of solutions in digital justice. This approach facilitated the development of an applied framework that translates AI system outputs into a system of measurable evidentiary indicators and data provenance verification scenarios, thereby ensuring the legitimacy of technology use in criminal proceedings.

To assess the real-world impact of technologies on investigations, a case-study method was applied to five key technological systems. These systems are officially integrated into the operations of the Singapore Police Force (SPF) and financial intelligence units, represent various automation modalities (AI/Machine Learning (ML), Robotic Process Automation (RPA), video analytics, sensor systems), and generate digital artefacts potentially relevant to the evidentiary framework. The following were analysed: SATIS+ (Commercial Affairs Department (CAD)/ Anti-Scam Command (ASCom)): a platform for streamlining the detection of elements that facilitate scams; Project Automation of Scam-fighting Tactics & Reaching Out (A.S.T.R.O.) (CAD/ASCom): RPA automation for data exchange and mass Short Message Service (SMS) alerts (Singapore Police Force, 2024a); and the Scam Analytics and Tactical Intervention System (SATIS): AI/ML triage and disruption of fraudulent web resources (SPF + partners) (Singapore Police Force, 2024b). Also utilised were the detection of stolen vehicles via Automated Number Plate Recognition (ANPR) in the Next-Generation Fast Response Car (NG-FRC), and Q-Crowd Counter (SPF + HTX): AI video analytics for crowd counting from drones (Singapore Police Force, 2024b). The technologies were analysed according to three universal criteria for legal assessment: reproducibility, auditability, and explainability, with an additional examination of the output type (candidate signal vs. evidentiary impact) and the presence of control artefacts (logs, versioning, data integrity, provenance/verification for GenAI). This was undertaken to operationalise the legal assessment of algorithmic systems by identifying their digital artefacts and the threshold of procedural guarantees depending on the output's status (signal or evidentiary impact).

The normative-analytical analysis method was employed to systematise the logic for evaluating electronic data, which distinguishes between the technical admissibility of evidence in a case and algorithmically generated results in Singapore's criminal process. This was based on the trial court judgment Magistrate's Appeal No. 9043 (2024) and the appellate court judgment Court of Appeal No. 42 (2025). The selection of these judgments was determined by the fact that, together (first instance and appeal), they crystallise the doctrinal logic for evaluating electronic data. For each source, the object of regulation/context, key procedural function, minimum conditions for use in evidence, and significance for AI/ML outputs were identified. This enabled the determination of criteria for the procedural admissibility of algorithmic results and the requirements for the explainability of the method by which they were generated.

Based on the foregoing, a risk-oriented normative-analytical approach was applied, aimed at formalising the minimum procedural requirements for the use of algorithmic outputs in the criminal process of Singapore. To identify relevant risk categories, the official report in the case of Originating Claim No. 125 (2025) was used as a methodological guide, allowing for the modelling of potential procedural consequences arising from the use of unverified algorithmic materials. The selection of this specific case was determined by its representativeness concerning the consequences of submitting GenAI-assisted materials containing unverified or false citations. This facilitated a comparison of the identified risks with Singapore's regulatory and institutional benchmarks and the operationalisation of the derived requirements into a list of control procedures to ensure contestability, verifiability, and procedural good faith. A limitation of this study is the reliance on open reports and public descriptions of systems, which typically do not include full technical model metrics, detailed validation protocols, or internal technical audits. Due to limited access to source code and proprietary algorithms, the technical reliability of the systems was analysed primarily through the lens of governance logic and the requirements of procedural verifiability, rather than through a comprehensive set of empirical performance indicators.

Results

Architecture and applied use of algorithmic systems in criminal law enforcement

AI automates cognitive tasks (classification, prediction, pattern detection), and ML, as a subset of AI, derives rules from data; consequently, its results are probabilistic and necessitate quality testing, drift monitoring, and documentation of limitations. For legal assessment, the key factors are not technology "labels", but the reproducibility, auditability, and explainability of outcomes. Although RPA is deterministic, its scalability also requires logging, access control, and error management. GenAI generates novel content and carries specific risks (hallucinations, provenance issues); therefore, in criminal investigations, it should be used only in a supporting capacity and with enhanced verification (Personal Data Protection Commission, 2020). In practice, AI-driven analytics produce "candidate" signals (anomalies, risk rankings, potential links) that require independent confirmation. When an algorithmic result is used as evidence or influences an evidentiary construct, the requirements for verifiability/reproducibility, explainability, error characterisation, and procedural audit (versions, logs, data integrity) are heightened (Personal Data Protection Commission, 2020).

For GenAI, additional critical requirements are established, including enhanced verification of materials prior to submission to court, the prevention of misleading the court, and an emphasis on ensuring provenance, transparency, and incident management as necessary conditions for building a trustworthy ecosystem (AI Verify Foundation, 2024). The implementation of these standards entails: enhanced verification – the user's obligation to personally verify each output for factual errors and "hallucinations", as the probabilistic nature of the technology does not guarantee automatic accuracy; procedural good faith – the mandatory disclosure of AI application and a guarantee that the generated content is not presented as authentic primary data, to avoid misleading the court; provenance and transparency – the implementation of methods to identify content sources (digital watermarks, metadata), allowing for traceability of the method and conditions of material creation; incident management – the existence of clear protocols for responding to instances where the system produces incorrect or harmful results, which is a prerequisite for the stability of the legal framework (Infocomm Media Development Authority, 2024).

In the criminal justice context of Singapore, the application of AI and analytics is best described as a chain: "data → processing → forensics → procedural verification". The SPF should be regarded as the primary operator within the system: the police initiate the collection/processing of large (streaming) datasets, utilise analytics to support operational decisions, and generate primary digital artefacts – records, event logs, automated calculations, alerts, and other machine-generated results (Singapore Police Force, 2024a). From an evidentiary perspective, the very fact of technological advancement increases the volume and significance of digital traces in a case, but does not automatically render them evidence. Their procedural status only emerges after proper documentation of provenance, ensuring integrity, and enabling verifiability – following the "translation" of an operational product into evidentially admissible material, which depends on subsequent links in the chain (forensics/judicial standards).

Within Singapore's criminal justice ecosystem, the Evidence Act of the Republic of Singapore (1997) serves as the fundamental regulator, transforming "raw" digital traces into evidentially admissible material. Analysis of the Act reveals three critical mechanisms in this transformation. The Act establishes legal presumptions that streamline the prosecution's burden of proof. The court presumes that a device or process which ordinarily produces an electronic record was functioning correctly, unless proven otherwise. This is crucial for automated recognition systems, as it allows their primary records (photos/video) to be admitted automatically without a technical audit of every single camera on each occasion. For an AI's operational output to attain the status of evidence, it must undergo identification and authentication procedures. According to the Evidence Act of the Republic of Singapore (1997), the critical conditions are: documenting provenance (clearly recording the source of the record and the conditions of its acquisition), ensuring integrity (demonstrating that the data was not distorted during transmission or algorithmic processing), and correctness of reproduction (confirming that the material presented to the court is identical to the original machine record). The distinction between the admissibility of a record and the reliability of its interpretation is the most critical aspect of the Act concerning AI technologies. The Evidence Act primarily addresses the question of admissibility – the very fact of an electronic record's "entry" into a court case. The mere existence of a record (for example, a "match" generated by a facial recognition system) and its authenticity do not automatically imply the reliability of its substantive conclusion. The Act only provides "procedural entry", whereas the reliability of interpretation (whether this "match" is indeed accurate) requires separate justification through the stability of the method and a description of the algorithm's error rates. The Evidence Act transforms the operational output of an AI system into evidentiary material through a rigorous "translation" procedure, where the technical output is supplemented by event logs, metadata, and a description of the processing method. This ensures that automated conclusions are not accepted by the court unconditionally, but are subject to independent verification and challenge (Evidence Act of the Republic of Singapore, 1997).

The Commercial Affairs Department (CAD) is institutionally the most "natural" environment for analytics and automation, as financial crimes and fraud typically possess a networked and transactional structure (chains of transfers, linked accounts/identifiers, digital communication channels) where manual analysis becomes a bottleneck. Therefore, the CAD logic of technological

adoption reduces to two complementary modes: the analytical mode – data integration and advanced analytics to identify patterns, connections, and prioritise subjects of interest, where algorithmic results generally constitute "candidate" hypotheses (to be investigated further) rather than final conclusions; and the operational-automated mode (RPA/scaling interventions) – automating response/prevention procedures, where the effect is achieved through scale and speed (Magistrate's Appeal No. 9043, 2024). This implies that within CAD, technologies simultaneously enhance the investigative function (more quickly finding relevant connections) and bolster the preventive/operational function (scaling interventions). At the same time, this is where the risk-paradox of automation is most evident: incorrect configurations, data errors, or methodological limitations scale just as rapidly as the positive effects. Hence the practical demand for accountability: logging, reproducibility, and the ability to explain why the system highlighted a particular object and what the margins of error are (Personal Data Protection Commission, 2020).

The HTX performs not merely a supporting role, but a structural one: the agency ensures the design, implementation, support, and development of technological solutions for the Home Team, including AI and analytical capabilities. For the topic of evidence, the key point is not that HTX "creates tools", but that it determines the technical characteristics of the artefacts which subsequently circulate in the criminal process: what exactly is logged, how versions are recorded, how processing procedures are described, whether auditing is possible, and how integrity is ensured. Within the Digital & Information Forensics domain, (Home Team Science and Technology Agency, 2025) transforms "raw" digital data into practically usable results for institutional application. It is here that typical procedural risks concentrate: version control of tools, reproducibility of procedures, data integrity control, documenting the chain of processing, and methodological limitations. HTX should be interpreted as a link that can either enhance evidentiary reliability (through standardisation and audit) or create a "black box" if control mechanisms are insufficient (Guide on the Use…, 2024).

The judicial system acts as a procedural filter; even with active technological adoption by police/agencies, the integration of results into the judicial framework is only possible within the standards of fairness and verifiability. On one hand, the digitalisation of court services and procedures creates an environment where electronic materials are the norm. On the other hand, courts explicitly delineate the boundaries for using Generative AI (GenAI): it is permitted as an assistive tool, but the user bears responsibility for the accuracy, relevance, and correctness of the submitted material; enhanced scrutiny is expected, and misleading the court is unacceptable. Courts effectively enshrine the principle that technology may support the preparation of materials but cannot substitute procedural safeguards (verification, transparency, accountability) (Guide on the Use…, 2024). The institutional landscape of Singapore's criminal justice ecosystem appears as follows: SPF/CAD generate demand and produce digital artefacts (operational and analytical), HTX determines their technical quality and forensic suitability, and the Singapore Courts set the threshold for procedural admissibility (particularly for GenAI content). This multi-layered structure explains why, in criminal investigations, the key factors become not only the accuracy of the algorithm but also the distribution of responsibility among institutions, the auditability and reproducibility of the data processing chain, and the possibility of procedural challenge and verification of results. Furthermore, this ensures a comparable description of scenarios and establishes the conditions for verifiability, reproducibility, and procedural accountability, summarised in Table 1.

Table 1. Applied scenarios of AI/analytics utilisation in Singapore's criminal investigations

Technology	Data (Input)	System Output	Characteristics	Risks/Vulnerabilities
Stolen Vehicle Detection via ANPR in NGFRC (SPF)	Number plate images/ video feed + database of "target" technical specifications (matching logic)	Automatic "number match" alert → subsequent procedural actions leading to arrest and prosecution for vehicle theft	Accelerated object identification, reduced reliance on random "human" observation, increased likelihood of prompt apprehension	False positives (reading errors, character ambiguity), risk of "tunnel vision" after the alert, reproducibility issues (algorithm settings/ version, thresholds)
SATIS: AI/ML Triage and "Disruption" of Fraudulent Web Resources (SPF + partners)	Indicators/signals of suspicious websites (domains/content/ complaints/patterns)	Systematic triage/ assessment → swift blocking/neutralisation, outcomes reported as mass "disruptions" of channels/ websites	Scaled preventative response, reduced time between resource emergence and intervention, prioritisation of objects for investigative actions	Risk of misclassification, complexity in explaining criteria, potential impact on third-party rights, evidentiary vulnerability without validation/audit protocols
SATIS+ (CAD/ ASCom): Platform for "Streamlining" Detection of Fraud-Facilitating Elements	Online monikers, phone numbers, bank accounts, e-wallets/ virtual accounts, crypto addresses	Triage → managerial/ legal actions; over 7,200 monikers triaged and over 3,700 directives issued under the Online Criminal Harms Act (OCHA)	Single collection point for consolidating signals, faster scaling of response and linking entities (account – account – number – address)	False "linking" of entities, automated error propagation across sources, opacity of triage rules for third-party verification

Continued Table 1

Technology	Data (Input)	System Output	Characteristics	Risks/Vulnerabilities
Project A.S.T.R.O. (CAD/ASCom): RPA Automation for Data Exchange and Mass SMS Alerts	Data from banks/suspicious transactions/accounts (information exchange), lists of potential victims, information processing and dissemination workflows	Automated account referrals + SMS alerts; 8,580 accounts and 777,170 SMS sent to 55,609 individuals; potential prevention of losses amounting to $420.41 million	Drastic acceleration of intervention, scalability without proportional increase in human resources, "harm prevention" effect through early notification	Data quality risks (false suspicions), automation/routing errors, questions regarding legal basis for processing/sharing and proportionality of intervention
Q-Crowd Counter (SPF + HTX): AI Video Analytics for Crowd Counting from Drones	Real-time video stream from UAVs	Crowd size estimation for situational management during an event	Real-time environmental analytics, enhanced situational awareness, tool for response planning	Risks of inaccurate estimations in complex conditions (angles/occlusion), privacy and proportionality of surveillance

Note: UAV – Unmanned Aerial Vehicle
Source: compiled by the author based on Singapore Police Force (2024a; 2024b)

The application of AI/analytics in Singapore's criminal investigations is primarily implemented in two functional modes: an alert-triage mode, where systems generate signals about potentially relevant objects or resources (ANPR/NGFRC, SATIS, SATIS+); and an operational-intervention mode, where automation supports scalable response actions or harm prevention (Project A.S.T.R.O., blocking/neutralisation in SATIS) (Singapore Police Force, 2024a; 2024b). Regardless of the specific technology, the system "output" takes the form of a decision-support suggestion or a management tool, rather than self-sufficient evidence. Consequently, the procedural relevance of such results depends on the ability to document and verify their origin and the parameters of their generation. Common vulnerabilities recur across cases: risks of false positives/classifications, opacity of criteria, errors in integration and entity "linking", as well as the amplification of consequences through automation. Accordingly, to minimise procedural risks, standardised mechanisms for logging, version control, documenting thresholds/settings, describing errors, and ensuring independent verification are critical, taking into account specific requirements of proportionality and privacy for surveillance-based solutions (video analytics).

During the commissioning of the NGFRC, the ANPR function in June 2024 facilitated the detection of a stolen vehicle during patrol, leading to the arrest and subsequent prosecution of the driver (Singapore Police Force, 2024b). From an evidentiary perspective, the ANPR alert serves as the basis for subsequent procedural actions, whereas the potentially relevant evidentiary materials are the primary number plate images/video, metadata (time, location, camera/platform identifier), as well as event logs concerning the generation of the "match" and subsequent actions (Evidence Act of the Republic of Singapore, 1997). Procedural admissibility here is determined not by the fact of the "match" itself, but by the ability to reconstruct the chain: input data → algorithmic operation → human verification/decision → action, with the typical point of challenge being the reliability of identification (image quality, reading errors, thresholds/version of the tool).

SATIS (Singapore Police Force, 2024b) is presented as an AI/ML-based tool for triage and supporting measures to neutralise scam-related web resources. Within the evidentiary framework, the most relevant are the primary digital traces upon which the assessment is based (domain/hosting attributes, content artefacts, records of reports/complaints, technical logs), whereas the algorithmic triage typically performs the function of analytical justification for initiating actions. If triage is used to support actions (blocking/disruption), its procedural role is contextual. However, if it is used to confirm the "nature" of a resource, the need arises to disclose the evaluation parameters, errors, and validation procedures; otherwise, the result possesses limited verifiability as an electronic record (Evidence Act of the Republic of Singapore, 1997).

SATIS+ (Singapore Police Force, 2024a) is described as a platform to support the identification/neutralisation of fraud-facilitating elements (online monikers, phone numbers, accounts, alternative payment instruments, and crypto addresses). Procedurally relevant are the primary records from sources substantiating the links between entities (including documented traces concerning accounts/transactions/identifiers), as well as a reproducible chain of data provenance and the conditions of their processing. In contrast, the triage output is an analytical result, and the directive is an act of regulatory response, which may be relevant for the chronology and grounds of intervention but does not substitute for proving the elements of a criminal offence with primary evidence (Evidence Act of the Republic of Singapore, 1997). The key procedural vulnerability of SATIS+ is associated with entity "linking"; therefore, the minimum requirements for verification are documented sources for each attribute, linking rules, and the ability to reconstruct which specific data led to a particular link/directive.

Project A.S.T.R.O. (Singapore Police Force, 2024a) utilises RPA to automate information-sharing, information-processing, and the mass dissemination of SMS alerts.

In criminal proceedings, such materials are significant for confirming the fact, time, and sequence of actions performed (message dispatch, script execution, information exchanges). Potential evidentiary materials include message dispatch/delivery logs, referral records, and internal logs of automation script execution (Evidence Act of the Republic of Singapore, 1997). Since RPA is rule-based, procedural verification focuses on reconstructing the rules and execution logs (which rule was triggered, on what data, and when), as well as on the legal bases for processing/sharing and the proportionality of intervention; without this, scalability complicates the individual verification of correctness.

Q-Crowd Counter (Singapore Police Force, 2024b) – is an AI tool for real-time video data processing from UAVs, used for estimating crowd size within the operational management of mass events. From an evidentiary perspective, the automated estimation of the number of people has limited independent significance, whereas the potentially relevant evidence could be the primary video recording (subject to metadata, integrity, and a documented chain of custody) (Evidence Act of the Republic of Singapore, 1997). If the count result is used in a case, it must be procedurally linked to the primary video (with identification of the segment, time, processing parameters) and be subject to verification of the margin of error under the specific recording conditions; otherwise, only the primary recording remains suitable for verification.

The described cases indicate that AI/analytics and automation in Singapore are applied primarily for detection, prioritisation, and rapid response. Their connection to evidence is largely indirect: the algorithmic output forms the basis for action and directs the line of inquiry, whereas within the judicial framework, the primary digital records, metadata/logs, and the chain of custody are determinative. The more a party's position relies on an algorithmic inference, the higher the requirements become for explainability, logging, reproducibility, and the accessibility of materials for independent verification and challenge. Empirically (according to Singapore Police Force reports, 2024a; 2024b), the application of AI/analytics is concentrated in two areas: operational detection and situational response support (ANPR, video analytics) and scalable anti-scam/financial analytics and automation. The evidentiary vector in these cases is typical – AI/analytics generates triggers/leads/prioritisation, whereas the primary evidentiary weight is carried by primary digital records (video, logs, transactional and telecom data) along with a properly documented chain of custody. The 'AI output' acquires procedural significance only under conditions of its verifiability and contestability. For electronically or machine-generated materials, the decisive factor is not merely the existence of a record, but the substantiation of the reliability of its interpretation, the context of its creation, the method/settings, limitations, event logs, and the possibility of reproducing the result.

Procedural relevance and normative regulation of algorithmic results

To transition from the operational use of AI/analytics to their procedural relevance, it is necessary to distinguish between the conditions for introducing an electronic record into the evidentiary basis (authenticity/origin/correctness of reproduction) and the conditions under which an inference derived from this data can be considered reliable for proving a specific fact. It is precisely this distinction, between the admissibility of a record and the reliability of its interpretation, that structures the normative and judicial guidelines presented in Table 2.

Table 2. Normative and judicial guidelines for assessing electronic and algorithmically generated data in Singapore's criminal

Judicial Guideline	Subject of Regulation / Context	Key Procedural Function	Minimum Conditions for Use in Evidence	Significance for AI/ML Outputs and Algorithmic Results
Evidence Act (Cap. 97) (including presumptions regarding electronic records) (Statute)	Electronic records and data: establishing authenticity, origin, correctness of reproduction/transmission, presumptions regarding the operation of the device or the process of creating/transmitting records	Provides procedural mechanisms for introducing electronic materials into the evidentiary basis (identification of electronic record, authentication, origin, correctness of reproduction)	Proper documentation of the record's source, conditions of acquisition/storage, connection to the relevant device/process, and the possibility of reproduction/verification within the proceedings	Defines the conditions for the admissibility and authenticity of electronic materials, but does not automatically establish the reliability of substantive inferences drawn from algorithmic data processing
SGHC 287 (2024) (Case Law) (First Instance)	Use of data from a wearable device (smartwatch) to corroborate factual circumstances	Distinguishes between the procedural admission/identification of electronic data and the assessment of its suitability to substantiate a specific fact	Beyond confirming the existence and origin of the record, it is necessary to substantiate the technical/methodological suitability of the data for the relevant inference (conditions of formation, limits of applicability, margin of error, stability)	Algorithmically generated measurements/classifications require separate substantiation of reliability as a basis for factual conclusions SGCA 21 (2025) (Case Law (Appeal))

Continued Table 2

Judicial Guideline	Subject of Regulation / Context	Key Procedural Function	Minimum Conditions for Use in Evidence	Significance for AI/ML Outputs and Algorithmic Results
SGCA 21 (2025) (Case Law (Appeal))	General approach to assessing electronic data in evidence, using data from a wearable device as an example	Articulates a fundamental distinction: the authenticity of an electronic record and the correctness of its acquisition are not equivalent to the reliability of its interpretation for proving a fact	For the evidentiary use of an inference derived from electronic/algorithmic data, grounds for trusting the method are necessary: an explanation of how the result was generated, its limitations, potential errors, reproducibility, and the possibility of independent verification/challenge	Establishes the requirement: the greater the evidentiary reliance on algorithmic output (match/score/triage), the greater must be the transparency of parameters, version control, logging, and the possibility of verification

Source: compiled by the author based on Evidence Act of the Republic of Singapore (1997), Magistrate's Appeal No. 9043 (2024), Court of Appeal No. 42 (2025)

Table 2 summarises the two-tiered logic for evaluating electronic and algorithmically generated data in Singapore's criminal procedure. At the statutory level, the Evidence Act ensures the procedural 'entry' of electronic records into the evidentiary basis through mechanisms of authentication, presumptions regarding origin, and correctness of reproduction; that is, it primarily addresses the issues of identification and admissibility of the record. At the level of case law Magistrate's Appeal No. 9043 (2024), Court of Appeal No. 42 (2025), the focus shifts to the substantive suitability of the data for proving a specific fact: even with an authentic electronic record, a party must substantiate the reliability of the interpretation (the method of acquisition/classification, conditions of application, margin of error, limitations, and reproducibility), as well as ensure the possibility of independent verification and challenge. In practical terms, this means that AI/ML outputs (match/score/triage) cannot function as self-sufficient evidence solely on the basis of their documented existence: their evidentiary weight depends on the transparency of parameters, version control, logging, and the presentation of the method's limitations, enabling the court to assess not only the authenticity of the material but also the soundness of the inference drawn from it.

AI/analytics and automation are used in the law enforcement context primarily for operational support (detection, prioritisation, accelerating response times, processing large datasets). However, in criminal procedure, such operational effectiveness is not synonymous with evidentiary admissibility. The approach under the GIL requires a separate justification for the reliability of interpreting electronic/algorithmic data to prove a fact. Technical risks encompass false positive/ false negative results and the sensitivity of system outputs to data quality and structure (images/video; transactions; the evolution of criminal patterns over time). For triage/scoring approaches, data drift is significant, necessitating regular testing, monitoring, and documentation of application limitations. As public reports typically do not contain error metrics or complete validation protocols, the role of internal assurance procedures and the recording of parameters/versions becomes crucial (Personal Data Protection Commission, 2020). Governance risks arise from the organisational environment in which systems operate: multi-user access, integration with external sources, and updates to rules/scripts and configurations. For tools generating alerts/triage/lists/directives/referrals, critical elements include activity logging, change and version control, access differentiation, and traceability of incidents and corrections (Personal Data Protection Commission, 2020). In digital forensics, the governance component pertains to the procedural discipline of seizing, processing, preserving, and documenting digital artefacts, which determines the reproducibility and verifiability of results (Home Team Science and Technology Agency, 2025).

Legal/procedural risks materialise when an algorithmic outcome is used as a basis for establishing a fact. The approach under the GIL emphasises that the authenticity of an electronic record does not negate the need to prove the reliability of its interpretation. In practical terms, this entails three requirements: procedural rebuttability – the opposing party's ability to verify and contest the conclusion; disclosure of information – the availability of parameters, logs, versions, and methodological boundaries; and expert knowledge – the need for specialised knowledge to explain to the court the possibilities and limitations of the result. This is relevant for both ML/AI and rule-based automation if it influences procedurally significant steps (Evidence Act of the Republic of Singapore, 1997). Data and privacy risks are associated with processing large volumes of transactional, identification, and communication data, and their exchange, which increases the likelihood of unauthorised access, breaches, and function creep. Within governance logic, this aligns with requirements for data management, access control, data minimisation, and accountability throughout the system's lifecycle (Personal Data Protection Commission, 2020). Generative AI risks lie in the potential to generate formally correct but factually inaccurate content (including incorrect or fabricated citations), which is procedurally sensitive in court submissions. Guidelines for the responsible use of GenAI

have been established by the Singapore Courts (Guide on the Use…, 2024) and are encapsulated in the principle that using GenAI does not absolve a party from responsibility for the accuracy of filed materials and the duty of proper verification prior to submission.

Case law further affirms the procedural significance of this standard: in instances where GenAI-assisted document preparation leads to the submission of unverified or erroneous citations, this may result in procedural consequences for the party or their representative. The broader context of the digitalisation of court services does not alter these requirements but rather underscores the necessity of maintaining standards of honest submission of materials in a digital environment (Singapore Courts, 2024). The case of Originating Claim No. 125 (2025) serves as a key judicial reference, crystallising the position of the Singapore judiciary regarding the risks of generative artificial intelligence "hallucinations". The court's decision establishes a fundamental principle: technological assistance does not negate individual procedural responsibility. The court meticulously analysed the issue of the probabilistic nature of GenAI tools, which are capable of generating linguistically coherent but factually incorrect citations to precedents. It was established in this case that submitting documents with non-existent citations undermines the duty of candour owed to the court. The legal authenticity of a submission rests upon the verifiability of its sources, not merely the formal persuasiveness of the text. A critical aspect of the ruling is the affirmation that the legal counsel or party to the proceedings serves as the "final filter". The court emphasised that AI is not a legal entity and cannot bear responsibility for errors; delegating legal research to an algorithm without subsequent human verification (human-in-the-loop) constitutes professional negligence, and the use of AI is not considered a mitigating factor in the event of misleading the court. The case of Originating Claim No. 125 (2025) established a clear list of consequences for the improper use of GenAI: procedural disqualification of materials (the court has the right to disregard or strike out submissions containing unverified data); financial penalties (imposing on a party the obligation to cover costs incurred by the court and the opposing party due to the need to verify "fake" citations); and disciplinary oversight (referral to relevant regulatory bodies for breaches of professional ethics standards). This precedent elevates the Singapore Courts (2024) guidelines from the realm of recommendation to that of mandatory requirement. This means that every statement prepared with the assistance of AI must be traceable to a primary source verified by a human. Law firms and law enforcement agencies are obliged to implement internal verification protocols (cross-checking) before submitting any AI-assisted materials. The case of Originating Claim No. 125 (2025) stimulates the requirement for open declaration of GenAI use in procedural actions to enable proper risk assessment by the court. This demands that system operators and legal professionals ensure not only the technical functionality of the tool but also complete transparency regarding the method of verifying its outputs.

Therefore, it is advisable to ensure comprehensive logging and audit trails (audit logs), including the recording of user actions and system events (creation/export of results, views, configuration changes, integration exchanges). This facilitates, if necessary, the reconstruction of the chain "data → algorithmic output → procedural decision/action" and ensures the verifiability of the origin and integrity of materials. The implementation of version control for models, rules, scripts, and configurations is necessary to establish which specific version of the tool (including thresholds and parameters) was operative at the time a particular match/triage/referral was generated, as well as who made changes and when. Control points for human verification (human-in-the-loop) should be distinctly defined for cases where algorithmic output may lead to significant procedural consequences, accompanied by standardised documentation of who performed the verification, based on what data, and what decision was reached. To mitigate the risks of technical degradation of results, it is advisable to mandate regular quality testing, validity assurance, and data drift monitoring, including the documentation of application boundaries and typical errors. A coherent policy on data governance, access controls, and security must be established, particularly concerning data minimisation, retention periods, incident response procedures, and requirements for inter-agency data exchange. These elements are fundamental in determining the stability and evidentiary admissibility of digital artefacts in subsequent proceedings.

In using GenAI in legal work, it is advisable to proceed from the presumption that the tool is assistive, and that responsibility for the content and correctness of submissions remains entirely with the participant in the proceedings; therefore, any material prepared with the use of GenAI must undergo mandatory verification of facts, citations, and references before submission to the court. In practice, this should be supplemented by internal controls that prevent the inclusion of unverified or erroneous references to precedents or sources, as case law demonstrates that submitting such materials may entail procedural consequences for the party or their representative. Confidentiality requires separate attention: inputting sensitive or procedurally significant data into GenAI tools is justified only if there are clear guarantees regarding the processing and storage of information, consistent with general data management requirements and judicial guidelines on the responsible use of GenAI. To ensure the procedural verifiability of algorithmic outputs, it is recommended to retain primary records and metadata (video/photo, transactional data, telecom logs, system journals) along with documented data provenance and the chain of custody/transmission. Furthermore, it is necessary to document the description of the method and the limits of application: what exactly the system does, under which conditions the result is correct, what typical errors and limitations are known, and how these are accounted for in practical use.

Discussion

The research findings demonstrated that within Singapore's law enforcement system, artificial intelligence is transforming from a tool for automating routine tasks into a multi-layered architecture for operational triage and decision support. The formation of functional modes (alert-triage and operational-intervention) enables law enforcement agencies to scale response measures, particularly in the fight against fraud, where algorithmic systems ensure the prioritisation of subjects of attention. This approach aligns with the conclusions of N. Lettieri *et al.* (2023), who theoretically substantiated the human-machine collaboration strategy as a means of overcoming AI's "blind spots", where the algorithm acts as an analytical filter, while the final procedural decision rests with the human. Concurrently, the emphasis on the need for independent verification and contestability of algorithmic conclusions, identified in this study, correlates with the concept of "contestable AI" in the work of F. Maoro & M. Geierhos (2025), where the transparency of semantic modelling is considered a key condition for making informed decisions in criminal intelligence. The transformation of AI into a multi-layered decision-support architecture confirms the shift towards a human-machine strategy, where the effectiveness of scaling response measures is combined with the critical necessity of transparency and human control to ensure the contestability and validity of procedural conclusions.

Research by T. Greene *et al.* (2022) showed that a key vulnerability of algorithmic risk assessment tools is their predictive inconsistency, arising from model sensitivity to the structure of input data. This confirms the "risk paradox" of automation identified in the current study: incorrect settings or data errors in systems such as ANPR or SATIS scale as rapidly as the positive effect of their implementation. The authors also emphasised the risks of "tunnel vision" when using predictive systems, which corresponds to the results of the analysis of Singaporean cases regarding potential bias and the need to account for errors when generating "match" signals. In this context, the conclusions of A.S. Almasoud & J.A. Idowu (2024) regarding algorithmic fairness in predictive policing reinforce the thesis that without regular monitoring of data drift and auditing of model parameters, operational efficiency may conflict with the principles of non-discrimination.

The work of T. Douglas *et al.* (2021) revealed that a fundamental condition for the effectiveness of algorithmic risk assessment tools in criminal justice is not only the mathematical sophistication of the models but also the quality and representativeness of the input data. The authors noted that a deficit of reliable data leads to systemic errors that are subsequently difficult to identify in "machine" conclusions. This correlates with the current study's findings on the functioning of ANPR and SATIS systems (Singapore Police Force, 2024b), where the "risk paradox" of automation was identified: incorrect settings or methodological limitations based on historical data scale as rapidly as the operational benefit of the system. Parallels between these studies indicate that the identified problems of decision dependence on data structure necessitate systemic audit and regular monitoring of data drift. Concurrently, R.A. Berk *et al.* (2022) proposed methods for improving the fairness of algorithmic assessments through conformal prediction, which aligns with the current study's conclusions on the need to transition from probabilistic AI "candidate" signals to independent human confirmation of each result (human-in-the-loop). The "risk paradox" of automation necessitates systemic audit and data monitoring to prevent the scaling of errors and guarantee algorithmic fairness.

Research by M.-P. Sandoval *et al.* (2024) and S.M. Qureshi *et al.* (2024) demonstrated that systemic threats from deepfakes to criminal justice arise from the difficulty of identifying manipulations in multimodal data. This correlates with the current study, which identified specific risks of Generative AI (hallucinations, provenance issues) that necessitate mandatory enhanced verification of digital materials before their submission to court. The authors also emphasised that the technical sophistication of deepfakes can undermine trust in digital evidence overall, which corresponds to the results of the analysis of Singaporean guidelines: GenAI technology may support the preparation of materials, but responsibility for their accuracy and correctness invariably rests with the user. Parallels between the results and the Singaporean case indicate that the use of unverified algorithmic results or fabricated precedents leads to real procedural consequences for parties and their representatives. This further substantiates the need for the evolution of the control system towards a model of institutionally formalised oversight over the entire data processing cycle, from the primary artefact to the court submission, as the sole condition for maintaining trust in digital justice. Ensuring institutional control over the data lifecycle, combined with the personal responsibility of the user, is a critical prerequisite for the legitimate use of Generative AI in criminal justice.

The findings established that, unlike purely operational systems, the evidentiary framework in Singapore is based on the structuring role of the HTX agency, which embeds control elements directly into the technical architecture of forensic instruments. The technical properties of artefacts (logging standardisation, model version control, and documentation of the processing chain) are determined at the design stage, enabling the transformation of "raw" digital data into procedurally admissible materials with guaranteed integrity. This approach correlates with the conclusions of D. Dunsin *et al.* (2024), who demonstrated that the integration of AI and ML in contemporary 21st-century digital forensics requires new standards of transparency and incident audit to maintain trust in investigation outcomes. Furthermore, the emphasis identified in this study on the necessity of content provenance traceability corresponds with the position of J. Loovens & H. Tinmaz (2025), who noted that amidst the growing threat from deepfakes, only systematic verification and transparency of processing methods allow for the preservation of the evidentiary value of digital

materials. The implementation of explainable AI and the standardisation of forensic procedures enable the transformation of the algorithmic "black box" into a transparent evidentiary tool, ensuring the procedural reliability of justice.

The research by D. Purves (2022) documented that the expansion of algorithmic policing carries ambiguous implications for the fairness of justice. On one hand, automation allows for the processing of vast information arrays; on the other hand, without robust accountability mechanisms, it can exacerbate discriminatory practices. This corresponds with the current study's findings regarding the alert-triage mode of operation of the SPF and CAD, where the scaling of anti-scam interventions (as in the A.S.T.R.O. project (Singapore Police Force, 2024a)) is accompanied by risks of misclassification and potential impact on the rights of third parties. The author also emphasised the need for transparency in selection criteria, which aligns with the requirements identified in the study for the explainability of algorithmic outputs and access to event logs for independent verification. Thus, the transformation of AI in Singapore into a multi-level decision-support architecture allows for the critical scaling of law enforcement measures; however, its safety depends on the implementation of a "human-in-the-loop" strategy and the prevention of the "risk paradox" of automation through systematic audit and control of data bias. The procedural reliability of algorithmic results is achieved through the introduction of explainable AI and institutional control over the complete data lifecycle, enabling the court to distinguish between the technical authenticity of a digital record and the validity of its intellectual interpretation.

Conclusions

The research findings established that RPA technologies, despite their deterministic nature, require equally strict logging and access control as AI, due to the risks of large-scale error propagation. The Singapore Police Force (SPF) acts as the primary operator of the ecosystem, initiating the "data → processing" chain and producing primary digital artefacts for investigations. The networked and transactional nature of contemporary 21st-century financial crime makes automation within CAD an indispensable tool for overcoming the limitations of manual analysis. The logic of technologisation in financial crime fighting units is based on distinguishing between the analytical mode of hypothesis generation and the operational-automated mode of rapid interventions. The HTX agency performs a structuring role, determining the technical properties of evidence (model versions, logging parameters) already at the design stage of law enforcement systems. Within the realm of digital forensics, HTX ensures the critical transformation of "raw" data into procedurally admissible results, ready for judicial use. The judicial system functions as a "procedural filter", admitting technological results only on condition that they meet standards of integrity and verifiability. Normative regulation (Evidence Act) provides only the "entry" of electronic records into the evidentiary base, but does not guarantee the reliability of substantive conclusions drawn by algorithms. Judicial practice formulates the requirement for the prosecution to substantiate the technical suitability and stability of the data acquisition method, not merely the fact of its existence.

The practical effectiveness of algorithmic solutions is confirmed by the successful use of ANPR systems for real-time detection of stolen vehicles and the large-scale application of SATIS and SATIS+ tools, through which over 7,200 suspicious objects were triaged. At the same time, judicial precedents, notably the case of Tajudin bin Gulam Rasul and Mohamed Ghouse v. Suriaya bte Haja Mohideen, demonstrate the real procedural risks of improper use of generative AI, leading to the submission of unverified materials and corresponding sanctions for the parties involved. These examples underscore that high operational effectiveness in Singapore is invariably accompanied by strict requirements for the verification of each automated inference. The contestability of an algorithmic inference in criminal proceedings directly depends on the disclosure of the system's parameters, event logs, and the limits of the applied analytical methodology. "Human-in-the-loop" mandates the documentation of the verifier's identity, the list of data used by them, and the justification for the decision made based on the AI. To enable independent verification, law enforcement agencies are obliged to preserve primary records and metadata alongside a detailed description of the method of their processing. Future research should usefully focus on developing standardised protocols for the judicial audit of algorithmic results and improving mechanisms for the traceability of digital material provenance to ensure the contestability and reproducibility of evidence in criminal justice, particularly in Singapore.

Acknowledgements

None.

Funding

None.

Author Contributions

R. Jurka conceived and supervised the study, designed the methodology, and conducted data analysis. The author also drafted and revised the manuscript.

Conflict of Interest

None.

References

[1] AI Verify Foundation. (2024). *Proposed Model AI Governance Framework for Generative AI: Fostering a trusted ecosystem*. Retrieved from https://aiverifyfoundation.sg/downloads/Proposed_MGF_Gen_AI_2024.pdf.

[2] Alibašić, H. (2025). Harmonizing artificial intelligence (AI) governance: A comparative analysis of Singapore and France's AI policies and the influence of international organizations. *Global Public Policy and Governance*, 5, 93-113. doi: 10.1007/s43508-025-00116-w.
[3] Allen, J.G., Loo, J., & Luna, J.L. (2025). Governing intelligence: Singapore's evolving AI governance framework. *Cambridge Forum on AI: Law and Governance*, 1, article number e12. doi: 10.1017/cfl.2024.12.
[4] Almasoud, A.S., & Idowu, J.A. (2024). Algorithmic fairness in predictive policing. *AI and Ethics*, 5, 2323-2337. doi: 10.1007/s43681-024-00541-3.
[5] Beltrão, G., Goh, S.T., Sousa, S., & Lamas, D. (2025). Community, identity & stability? Building trust in facial recognition systems for mass surveillance. *Journal of Responsible Technology*, 24, article number 100139. doi: 10.1016/j.jrt.2025.100139.
[6] Berk, R.A., Kuchibhotla, A.K., & Tchetgen Tchetgen, E. (2021). Improving fairness in criminal justice algorithmic risk assessments using optimal transport and conformal prediction sets. *ArXiv*. doi: 10.48550/arXiv.2111.09211.
[7] Chase, J., Phong, T., Long, K., Le, T., & Lau, H.C. (2021). Grand-vision: An intelligent system for optimized deployment scheduling of law enforcement agents. *Proceedings of the International Conference on Automated Planning and Scheduling*, 31(1), 459-467. doi: 10.1609/icaps.v31i1.15992.
[8] Court of Appeal No. 42 "GIL v Public Prosecutor". (2025, May). Retrieved from https://www.elitigation.sg/gdviewer/s/2025_SGCA_21.
[9] Douglas, T., Davies, B., Pugh, J., Brown, R., Hass, B., Forsberg, L., Mishra, A., Singh, I., Savulescu, J., & Fazel, S. (2021). *Algorithmic risk assessment tools in criminal justice: The need for better data*. Oxford: University of Oxford.
[10] Dunsin, D., Ghanem, M.C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, 48, article number 301675. doi: 10.1016/j.fsidi.2023.301675.
[11] Evidence Act of the Republic of Singapore. (1997, December). Retrieved from https://sso.agc.gov.sg/Act-Rev/97/Published?DocDate=19971220&ProvIds=pr76-.
[12] Greene, T., Shmueli, G., Fell, J., Lin, C.-F., & Liu, H.-W. (2022). Forks over knives: Predictive inconsistency in criminal justice algorithmic risk assessment tools. *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, 185(2), 692-723. doi: 10.1111/rssa.12966.
[13] Guide on the Use of Generative Artificial Intelligence Tools by Court Users. (2024). Retrieved from https://surl.li/elcwmu.
[14] Home Team Science and Technology Agency. (2025). *Digital & information forensics*. Retrieved from https://www.htx.gov.sg/who-we-are/what-we-do/our-expertise/digital-information-forensics.
[15] Infocomm Media Development Authority. (2024). *Singapore proposes framework to foster trusted Generative AI development*. Retrieved from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai.
[16] Khan, A.A. (2024). Reconceptualizing policing for cybercrime: Perspectives from Singapore. *Laws*, 13(4), article number 44. doi: 10.3390/laws13040044.
[17] Lee, H., & Lee, T. (2022). The tracetogether matrix has you – surveillance, rationalisation and tactics of governance in Singapore's COVID-19 app. *Platform: Journal of Media and Communication*, 9(2), 77-91.
[18] Lee, T., & Lee, H. (2020). Tracing surveillance and auto-regulation in Singapore: 'Smart' responses to COVID-19. *Media International Australia*, 177(1), 47-60. doi: 10.1177/1329878X20949545.
[19] Lettieri, N., Guarino, A., Zaccagnino, R., & Malandrino, D. (2023). Keeping judges in the loop: A human-machine collaboration strategy against the blind spots of AI in criminal justice. *Soft Computing*, 27, 11275-11293. doi: 10.1007/s00500-023-08604-z.
[20] Lim, N.F.-Z., & Tan, K.S. (2025). The new frontier: Regulating artificial intelligence in Singapore. *Singapore Academy of Law Journal*, 37, 436-463.
[21] Lim, S.S., & Chng, G. (2024). Verifying AI: Will Singapore's experiment with AI governance set the benchmark? *Communication Research and Practice*, 10(3), 297-306. doi: 10.1080/22041451.2024.2346416.
[22] Loovens, J., & Tinmaz, H. (2025). A systematic literature review of deepfakes in forensic science. *Forensic Imaging*, 43, article number 200647. doi: 10.1016/j.fri.2025.200647.
[23] Magistrate's Appeal No. 9043 "GIL v Public Prosecutor". (2024, November). Retrieved from https://www.elitigation.sg/gd/s/2024_SGHC_287.
[24] Maoro, F., & Geierhos, M. (2025). Contestable AI for criminal intelligence analysis: Improving decision-making through semantic modeling and human oversight. *Frontiers in Artificial Intelligence*, 8, article number 1602998. doi: 10.3389/frai.2025.1602998.
[25] Originating Claim No. 125 (Summons No. 1240 of 2025) "Tajudin bin Gulam Rasul and Mohamed Ghouse v. Suriaya bte Haja Mohideen". (2025, September). Retrieved from https://www.elitigation.sg/gd/s/2025_SGHCR_33.

[26] Personal Data Protection Commission. (2020). *Model AI governance framework*. Retrieved from https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf.
[27] Purves, D. (2022). Fairness in algorithmic policing. *Journal of the American Philosophical Association*, 8(4), 741-761. doi: 10.1017/apa.2021.39.
[28] Qureshi, S.M., Saeed, A., Almotiri, S.H., Ahmad, F., & Al Ghamdi, M.A. (2024). Deepfake forensics: A survey of digital forensic methods for multimodal deepfake identification on social media. *PeerJ Computer Science*, 10, article number e2037. doi: 10.7717/peerj-cs.2037.
[29] Sandoval, M.-P., Vau, M. de A., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, 13, article number 41. doi: 10.1186/s40163-024-00239-1.
[30] Seng, D., & Mason, S. (2021). Artificial intelligence and evidence. *Singapore Academy of Law Journal*, 33, 241-279.
[31] Singapore Courts. (2024). Strengthening justice, safeguarding society. In *Singapore courts annual report 2023*. Singapore: The Judiciary.
[32] Singapore Police Force. (2024a). *CAD report 2024*. Retrieved from https://www.police.gov.sg/-/media/SPF/Media-Room/Publications/CAD-Report-2024/CAD-Report-2024.pdf.
[33] Singapore Police Force. (2024b). *A future-ready Singapore Police Force: Cyber and beyond*. Retrieved from https://www.police.gov.sg/-/media/SPF/Files/Publications/PDF/SPF-Annual-Report-2024.pdf.