THE HON. JUSTICE ISAAC LENAOLA, CBS
JUDGE OF THE SUPREME COURT OF KENYA AND
CHAIR OF THE ICT AND COMMUNICATIONS
COMMITTEE OF THE JUDICIARY

TOPIC: INTEGRATION OF ARTIFICIAL INTELLIGENCE (AI) IN EFFECTIVE CASE MANAGEMENT

A PAPER PRESENTED TO THE JUDICIARY OF UGANDA JUDGES ANNUAL RETREAT

DATE: 2ND – 4TH FEBRUARY 2026

VENUE: KAMPALA, UGANDA

1. INTRODUCTION

- Technology plays a critical role in advancing access to justice for all by addressing longstanding barriers, including the cost of litigation, geographic distance, procedural complexity, and delays within the legal system. The Kenyan Judiciary is currently operationalizing the *Social Transformation through Access to Justice (STAJ)* Blueprint, which champions access to justice for the common *mwananchi,* by, among other means, utilizing modern technological tools.

- The Kenyan Judiciary, similar to the Ugandan Judiciary, has, in the recent past, made great technological advancements through the integration of digital tools in the administration of justice processes. Platforms such as e-filing systems, virtual courts, and remote connectivity, the cause list portal, the case tracking system, online legal information platforms, and the e-judiciary mobile app, and automated transcription, among others, have contributed to improved inclusivity and efficiency in the delivery of justice, thereby enhancing transparency and accountability, strengthening public confidence in the justice system.

- In the recent past, Artificial Intelligence (AI), though unregulated, has emerged as the most used digital tool in the legal space**,** transforming how legal research and analysis are conducted and how legal services are delivered, managed, and accessed. In Kenya, for instance, AI technologies are increasingly being applied to legal research, transcription, case management, and document review.

- Whereas AI technology enhances efficiency by reducing time spent on repetitive tasks, improving accuracy in legal research and analysis, and supporting better decision-making. However, the adoption of AI in the legal sector raises important concerns relating to data protection, ethical use, algorithmic bias, hallucinations, and the need for adequate human oversight.

- It is against this backdrop that this Paper proposes **strategic, ethical, responsible, and controlled adoption of Artificial Intelligence (AI) as a supportive, non-decisional tool within the judicial process.** The responsible integration of AI remains essential to ensure fairness, transparency, and the protection of fundamental rights.

- **AI is not intended to replace judicial reasoning, discretion, or independence, but rather to augment judicial efficiency** in the organization, structuring, summarization, and retrieval of information, particularly in complex matters characterized by voluminous records, multiple parties, and interrelated legal and factual issues.

AI-GENERATED EVIDENCE: WHAT MUST PARTIES DISCLOSE

2. When a party relies on AI-Generated or AI-processed evidence, what minimum disclosures should Judges require to assess authenticity and integrity?

- Generative AI is a rapidly evolving modern technology, with an expanding range of freely available AI tools for public use. It is therefore essential for users to understand both the capabilities and limitations of the specific models they employ. The quality and reliability of outputs generated by AI chatbots depend largely on how the models are trained, the accuracy and credibility of their training data, and the quality of user prompts. Consequently, AI-generated responses may not always be drawn from authoritative or verified databases, underscoring the need for careful evaluation and human oversight when using such tools for legal research.
- Judges must be aware that, even when generative AI systems are used with carefully formulated prompts, the outputs being (text, audio, images, video, or analytical data) may be inaccurate, incomplete, misleading, or biased. In particular, certain AI tools may generate fictitious cases, citations, or quotations, or refer to legislation, scholarly articles, or legal authorities that do not exist, a phenomenon commonly described as “hallucination.” Additionally, such systems may provide incorrect or misleading interpretations of the law or its application, produce factual inaccuracies, or affirm the accuracy of information when prompted, even when the information is erroneous. These limitations underscore the necessity of rigorous human oversight, independent

verification, and the continued exercise of judicial discretion when engaging with AI-generated outputs in the legal decision-making process.

- Judges must remain cognizant of both the capabilities and inherent limitations of AI systems. Information generated should be independently verified, preferably through authoritative and human-validated sources, before being incorporated into judicial decision-making. Reliance on unverified AI outputs poses significant risks, including the potential for erroneous judgments, the perpetuation of injustice, and the erosion of public confidence in the judiciary. Ensuring rigorous verification and exercising judicial discretion are therefore essential to uphold the integrity, fairness, and credibility of legal processes in the context of AI-assisted case management.
- The evidentiary test, provided for under the Evidence Act, is still applicable even in cases alleging AI-generated pleadings and evidence. The burden of proof is on the person who asserts the existence of a fact, and tools such as models, name/version, prompts, input, logs, timestamps, and post-processing may be useful for the court to establish culpability, but do not shift the responsibility for verifying the authenticity of text, image, audio, or video submissions.
- Judges, in highly contentious cases with complex ICT issues, are encouraged to utilize internal ICT support to verify the documents or evidence before the court and invite *amici curiae* for independent ICT expert support.

2.1 Should the Judiciary adopt a standard "AI Evidence Annex" for e-filings, aligned to our electronic transactions and e-filing framework?
What is the right sanction if the annex is incomplete or an integrity check fails?

- The **"AI Evidence Annex"** refers to a distinct section or document appended to a report or project, in which a party discloses and documents the use of artificial intelligence tools in preparing the work. It serves as both evidence and a mechanism to ensure transparency, analogous to the role of plagiarism checks in academic or professional submissions.
- Integrating the "AI Evidence Annex" into the Judiciary's existing digital infrastructure would be a significant investment, both financially and institutionally. Given the rapid evolution of AI technologies, the system would

require ongoing updates and likely necessitate partnerships with external technology providers to maintain reliability and effectiveness.

- A clear, comprehensive Regulatory Framework on AI (AI Act, Regulations, and Policy), such a framework provides a nationally applicable, predictable standard, and transparent framework that has undergone public consultation/participation to incorporate the views of all stakeholders, including advocates, litigants, and researchers.

AUTOMATED DECISION-MAKING & DUE PROCESS

3. Where a public body or a private actor uses AI to make or materially influence a decision affecting rights (benefits, employment, credit, or services), what due process should courts look for?

- Simply put, **"AI is technology that allows computers or machines to think and act in ways that normally require human intelligence."**
- AI systems can *learn from data* by recognizing patterns; *understand language* through chatbots and voice assistants; *recognize images* through face recognition and scans; *make decisions or predictions*; and create content such as text, images, and music.
- However, with all these capabilities, AI lacks the human element, values, and qualities such as compassion, understanding, empathy, fairness and justice, responsibility, and accountability. It is purely data-driven and chatbot-controlled and thus unable to deduce these values.
- Judges should intervene when public bodies or private entities employ AI to make decisions or materially influence outcomes. For instance, public bodies such as the Kenya Refugee Affairs Secretariat, the Kenya Revenue Authority, or the National Government may use AI to process applications, conduct tax assessments, or allocate services. Similarly, private entities such as financial institutions, insurance companies, or recruitment platforms may rely on AI for loan approvals, claims processing, or candidate selection. In processes that inherently involve significant human judgment, such as applications for refugee status, conducting the procedure entirely through digital means, without a human interface or human oversight ("human in the loop"), carries a substantial risk of producing unjust outcomes. Ensuring that critical decisions retain an element of human

judgment is essential to upholding fairness, protecting rights, and maintaining public confidence in both administrative and judicial processes.

3.1 What evidence should a decision-maker present to prove that a human in the loop actually reviewed the case? & Should courts order a Data Protection Impact Assessment (DPIA) in high-risk matters?

- To prove that a human-in-the-loop (HITL) has genuinely reviewed an AI-assisted decision, a decision-maker should present documentation that demonstrates substantive, active engagement rather than passive approval. In high-risk matters such as immigration & refugee matters, recruitment, credit, healthcare, and law enforcement, courts should, and often do, expect a Data Protection Impact Assessment (DPIA) to demonstrate that risks were identified and mitigated.
- Evidence of **Human-in-the-Loop (HITL) Review** is essential to demonstrate that human reviewers do not merely "rubber-stamp" decisions generated by AI systems. To ensure substantive oversight, institutions should maintain comprehensive audit logs and user activity trails that document the specific actions taken by human reviewers during the decision-making process. Case-specific notes and rationales further provide insight into the reasoning applied to each case, while records of overrides or modifications document instances in which human judgment corrected or adjusted AI-generated recommendations.
- Incorporating a **"Human First" workflow**, where reviewers are required to make an independent assessment before viewing AI outputs, helps mitigate the risk of anchoring bias and ensures that human evaluation drives the decision rather than AI influence. Additionally, training records and qualifications should be maintained to confirm that reviewers have received specialized instruction regarding the AI system's limitations, potential biases, and known failure modes. Finally, performance metrics should evaluate reviewers based on the quality and accuracy of their decisions, rather than speed.
- Together, these measures provide evidence that human oversight is meaningful, accountable, and capable of safeguarding fairness, accuracy, and transparency in AI-assisted decision-making.

3.2 Should Courts order a Data Protection Impact Assessment (DPIA) in high-risk matters?

- Yes. Courts should, and in many jurisdictions already do, require a comprehensive Data Protection Impact Assessment (DPIA) Report for high-risk automated decision-making.
- The DPIA is required whenever processing personal data is likely to result in a high risk to individuals. Examples include systematic profiling, processing sensitive data, and large-scale public monitoring. The primary purpose of a DPIA is to compel the organization to identify, assess, and demonstrate how potential risks to data subjects have been mitigated. This includes detailing mechanisms for human oversight, ensuring that decisions influenced or made by AI systems are subject to meaningful human review. Courts and regulatory bodies do not accept DPIAs as mere "tick-box" exercises; rather, they expect a substantive, well-documented assessment that clearly explains the AI system's logic, identifies potential risks, and justifies the measures taken to mitigate them.
- Importantly, a DPIA is a living document that requires regular review and updates as technology evolves or the risk landscape changes. Where a DPIA identifies residual high risks that cannot be sufficiently mitigated, the organization must consult the relevant Data Protection Authority (DPA) before deploying the system. This approach ensures accountability, transparency, and the protection of individual rights in the deployment of AI technologies.

BIOMETRICS, DIGITAL ID & PROPORTIONALITY

4. When biometric verification (fingerprint/face/iris) is required to access services, what necessity and proportionality test should we apply, and what remedies are appropriate where exclusion or error is shown?

- Biometric verification is the security process of authenticating a person's identity by comparing their biological or behavioural traits with stored data. Common types of biometric verification include fingerprint scanning, face recognition, iris or retina scanning, voice recognition, signature verification, and keystroke patterns. The system captures your biometric data, converts it into a digital template, compares it with stored data, and grants or denies access.

- It is used for civic duties, such as voting in general elections, and in private contexts, including unlocking smartphones, banking and payment apps, airport security, workplace attendance systems, online exams, and identity checks. Biometrics is more secure than passwords, it is fast and convenient, and it reduces identity fraud.
- Kenya's IEBC, for instance, uses biometric data during voter registration and verification at polling stations, which prevents multiple voting and enhances the transparency and credibility of elections. When primary biometric data is unavailable during voting, the electoral body has a duty to revert to the manual register for authentication to ensure that no one is denied access and that all parties present are allowed to vote.
- Where exclusion or error is shown, the parties have recourse to an alternative authentication method (PIN or OTP); request manual verification, file an access denied report, appeal, update, or re-enroll biometric data.

4.1 How should courts weigh fraud-prevention goals against risks of exclusion or data misuse?

- Courts usually balance fraud-prevention benefits against human-rights risks by applying a proportionality and fairness approach. Courts assess the legitimacy of the goal by asking whether preventing fraud is a legitimate and important objective, examining proportionality, and then considering whether the measures used are proportionate.
- If fraud prevention is achieved at the cost of widespread exclusion, courts may find it disproportionate, to assess the risk of exclusion, the Courts pay close attention to whether people are wrongly denied access, the Impact on vulnerable groups for instance, the elderly, disabled, and rural populations, the availability of alternative verification methods, and whether systems that exclude eligible users without providing backup are deemed unfair.
- The Courts evaluate data protection and misuse risks, including how biometric data is stored, secured, and accessed; whether there are clear limits on use; the risks of surveillance, leaks, or secondary use; and whether weak safeguards increase constitutional risk. Courts favor systems that include clear mechanisms for appeal or review; transparency regarding how data is used; and accountability for errors or abuses. Courts also apply

human rights standards, on rights such as privacy, equality and non-discrimination, dignity, political participation, and access to services.

- In conclusion, courts should uphold fraud-prevention measures only where they are proportionate, minimally intrusive, well-regulated, and do not unjustifiably infringe on or endanger individuals' rights.

4.2 What interim measures can prevent harm during mass enrollments or system outages?

- During mass enrolments like voter registration and system outages occur, interim measures should focus on preventing exclusion, protecting rights, and maintaining service continuity while problems are resolved. Courts and regulators often expect, *firstly*, to allow alternative verification methods such as manual registers or paper lists, physical ID documents, PINs, OTPs, or supervisor overrides, which prevent people from being locked out due to technological failure. *Secondly*, use grace periods and provisional access, such as temporary enrolment or access passes, provisional voting, or service access; and later verification once systems are restored. *Thirdly*, suspend penalties and deadlines, including pause sanctions linked to failed enrolment; extend registration or compliance deadlines; and ensure that no one is punished for system errors.
- Regulators can:

i. deploy rapid-response technical support, including on-site technicians, backup servers, offline modes, and emergency maintenance protocols;
ii. Prioritize vulnerable groups, including the elderly, disabled, rural, or low-literacy users
iii. Provide assisted enrolment or mobile units;
iv. Communicate clearly and transparently, such as public notices explaining the issue, clear instructions on alternative processes, and updates on timelines for resolution.;
v. Strengthen data protection during outages, such as limiting emergency access to data, logging all overrides and manual interventions, prevent misuse under "emergency" justifications

- Lastly, the Judiciary can provide relief by issuing temporary court orders that allow flexibility and independent monitoring of interim measures.

DEEPFAKE, MISINFORMATION, AND URGENT RELIEF

5. What is the right threshold and procedure for granting urgent relief when parties allege AI-Manipulated audio/video (deepfake) in a high-stakes context (elections, commercial reputation, criminal matters?

- A **deepfake** is a type of synthetic media, including fake audio, video, or images, that is generated using AI technology and shared online. It portrays non-existent realities or events that have never occurred, often creating hyper-realistic digital forgeries that can seamlessly insert individuals into videos and images, making it appear as if a real person did or said something they never did. Deepfakes are common during the electioneering period, when videos of politicians appearing to deliver speeches they never made, or fake celebrity videos or voice recordings, or altered videos are used to manipulate the public.
- Deep-fakes are dangerous and have serious legal and social consequences because they spread false information to unsuspecting members of the public, damage reputations built over time, and influence elections or public opinion. When the public cannot verify the authenticity of a video or image, it can take a long time for the issue to be rectified, by which time, the public has moved on or been defrauded.
- **Misinformation**, on the other hand, is misleading or incorrect information that is shared without the intention to deceive. Misinformation includes sharing incorrect news on social media, believing and forwarding unverified rumours, and outdated or wrong health advice.
- When parties in a high-stakes contest, like a presidential election petition, allege deep-fake or misinformation, the Judges have a duty to urgently deal with the matter by satisfying themselves on whether there is:
  a. **Credible prima facie case -** the applicant must present plausible evidence that the media is likely AI-manipulated, and that the claim is not merely disputed or embarrassing. The Courts do not require full proof at this stage; only credible doubt is required. The Evidence presented may include:
     i. Expert affidavits from digital forensics or metadata analysis;
     ii. Platform flags or takedown notices;

iii. Inconsistencies in audio-visual synchronization;

iv. Proof of sudden anonymous dissemination

b. **Imminent and irreparable harm** - the Courts can look for harm that cannot be adequately repaired by damages, and is time-sensitive, for instance, during an election period, personal reputation, or the safety of a person. For instance, electoral interference, incitement to public disorder, and Reputational or professional destruction;

c. **On a Balance of convenience,** the Courts weigh the harm of allowing continued circulation *vis-à-vis h*arm to freedom of expression or public interest, issuing a temporary restraint is more likely if relief is narrow and reversible; and

d. **Public interest considerations -** urgent relief is favoured where the content threatens democratic processes, or it undermines trust in institutions, or it risks large-scale misinformation.

Example: The President of the United States of America, Donald Trump, and the President of the Republic of Kenya have repeatedly appeared on social media platforms placed in caskets.

In Kenya, Harrison Nyende Mumia was arraigned at the Milimani Law Courts on multiple counts of "false publication" under Section 22 (1) of the Computer Misuse and Cybercrimes Act, 2018. On allegations that: On 30 December 2025, he allegedly used social media accounts (including a pseudo Facebook account under the name Robinson Kipruto Ngetich and his own Instagram account) to post digitally generated images portraying President William Ruto as critically ill or deceased. These images were allegedly false and misleading, and the charges claim he knowingly published them despite knowing they were untrue.

5.1 Should we adopt a fast-track Authenticity Protocol (a neutral expert, hash checks, and model disclosures under protective orders)?

- Yes. Adopting a fast-track Authenticity Protocol is strongly recommended and increasingly critical as synthetic content (AI-manipulated media) evolves. 2025-26 data indicate that hyper-realistic content can easily bypass traditional detection, cause immediate, widespread harm, and erode trust in real time.
- This Protocol will ensure that courts, regulators, and organizations can respond quickly, reliably, and fairly to curb rapid viral spread, protect rights while preventing harm, build public trust, and prevent the spread of deep-fakes without waiting for full trials or lengthy forensic analysis.
- The fast-track Authentication Protocol may include immediate preservation measures, Emergency filing guidelines, Pre-approved expert pool, Interim

relief framework, verification checkpoints, and a clear appeals/review mechanism.

5.2 How do we balance speed, free expression, and evidentiary reliability?

- Speed, freedom of expression, and evidentiary reliability are competing interests that must be balanced. Courts and regulators may employ the proportionality and layered-response approach to balance speed, freedom of expression, and evidentiary reliability in cases involving AI-manipulated media (deepfakes). The complexity of the matter notwithstanding, they must act before harm spreads; speed is necessary to prevent irreparable harm, but they must not bypass safeguards.
- Deepfakes and misinformation can go viral in hours, causing reputational, electoral, or financial harm. There is therefore a need to maintain speed by fast-track filings and preservation orders, pre-approved expert panels for rapid verification, and temporary, narrowly tailored interim relief, for instance, temporary removal or labeling of content or temporarily pulling the content down.
- Freedom of expression ensures that remedies taken by courts don't become permanent silencing tools, and this can be protected by avoiding overly broad takedowns, which risk censorship of legitimate content or debate. To balance the competing interests, the Courts can make interim measures which are proportional and reversible, Limit scope: remove only verified false content, not entire accounts, and include public notice and opportunity for appeal or rebuttal
- The Evidentiary Test is designed to ensure the accuracy of the information; deep-fakes must rest on credible evidence to avoid punishing innocent parties. This can be achieved by preserving original files and metadata immediately, requiring expert forensic verification (independent and transparent), documenting findings for accountability, using multi-layer verification that is technical and contextual, and answering who posted? Intent? and timing.

COMPETITION AND ALGORITHMIC PRICING

6. At what point does the use of common pricing/revenue software (or shared non-public data) by competitors become evidence of

coordination, and what discovery orders should courts consider (vendor algorithms, data feeds, compliance controls)?

- This is a technical question that cuts across Law, Technology, and Economics/Finance.
- The Kenyan Judiciary has adopted a home-grown digital development approach, where our ICT experts, guided by our data and technological needs, develop digital platforms that are fit for purpose. To date, the e-filing, e-payment, and UADILIFU platform that is linked to the Case Management System for the registration of charge sheets.
- From our experience, our homegrown digital platforms offer: greater control and customization, data Sovereignty and protection, long-term efficiency and capacity building.

How should courts distinguish between data-driven optimization and hub-and-spoke collusion?

- Courts usually distinguish lawful data-driven optimization from illegal hub-and-spoke collusion by focusing on independence, information flows, and intent, rather than on the mere use of common technology.

What interim conduct remedies (e.g., stop using non-public competitor data) are feasible pending trial?

- Interim remedies may include, top using non-public competitor data, firewalls, and data segregation, disabling or modifying algorithmic features, a human-in-the-loop requirement, limits on vendor conduct, data minimization and time delays, transparency and reporting obligations, preservation (not destruction) orders, and what courts usually avoid at the interim stage

JUDICIAL ETHICS & THE COURTS' OWN USE OF AI

7. What boundaries should guide judges, registrars, and advocates when using generative AI, and what training do we need across the Bar and the Bench?

- AI in Judicial Decision-Making, also known as "artificial reasoning," is a real concern for all justice actors. We reiterate that **AI is not intended to replace judicial reasoning, discretion, or independence but rather to augment judicial efficiency in organizing, structuring, summarizing, and retrieving information, particularly in**

complex matters characterized by voluminous records, multiple parties, and interrelated legal and factual issues.

- There are credibility challenges that are posed by the increasing presence of AI within judicial work. The key consideration for any judicial officer should be:
    i. **Opacity of Modern AI systems** - Judicial decisions are expected to be reasoned and explainable, the legitimacy of the outcome not only on what is decided, but on the ability of the parties and the public to understand why it was decided. Many AI systems operate in ways that may currently be incompatible with this requirement. They do not reason from legal principles or justify conclusions in the manner required under the law;
    ii. **Hallucinations and Integrity of Legal Material** - when used for legal research, AI can fabricate cases, citations, and quotations that appear convincing but are entirely false. Human oversight is extremely necessary to verify the AI output;
    iii. Other factors to be considered include bias and discrimination, impartiality, and the nature of Judging, judicial Independence and the hidden Influence and human values, judgment, and practical wisdom.
- **What do we need to do?**
    i. Joint Continuous training and capacity building programs, by the Judiciary Academy and Law Society;
    ii. Partner with Academic Institutions and Universities that are focused on modern technology;
    iii. Equip and engage the ICT department of the Judiciary; and
    iv. Beware, at all times, that ICT offers support not the solution.

7.1 Should we issue a short Practice Direction on AI use by the Courts and Counsel (including a ban on unverified AI citations)

- Recognizing that the national government, through the Kenyan Ministry of ICT (Ministry of Information, Communications & the Digital Economy), offers guidelines and policy direction on Artificial Intelligence (AI), and support, guidelines, and direction on ICT adoption to other government agencies;

- Recognizing the complexity and ever-evolving nature of modern technology and AI in particular, the Kenyan Judiciary developed the draft Kenyan Judiciary AI Policy that is currently undergoing public participation;
- From international best practices guided by countries such as Hong Kong (*Guidelines on the Use of Generative Artificial Intelligence for Judges and Judicial Officers and Support Staff of the Hong Kong Judiciary"*), the United Kingdom (*Artificial Intelligence: Judicial Guidance*, 2025"), and Ghana, which is also developing a national AI strategy.
- It is my considered opinion that this is the preferred route to regulating AI, as it brings together all stakeholders in the justice sector, as opposed to a short Practice Direction.

What Capacity-Building (templates, checklists, model orders) would help chambers handle AI issues consistently?

- The Judiciary should work with key stakeholders, including Parliament, Law Society, and academia, to enact a comprehensive Legal Framework on AI (AI Statute, Regulations, and Policies).
- Kenya is currently developing the draft Kenyan Judiciary AI Policy, and thereafter the regulations and lastly an Act of Parliament.

CONCLUSION AND WAY FORWARD

Modern technology, and AI in particular, has the potential to significantly transform the judiciary by improving efficiency and effectiveness. AI tools assist Judges with legal research and case management, thereby reducing backlogs and other administrative bottlenecks. When used responsibly, AI tools can support more informed decision-making, expedite judicial processes, and enhance transparency. In the use of AI:

1. Judges must recognize that judicial reasoning, independence, and accountability cannot be replaced by technology. AI tools are designed to support the administration of justice, enhance efficiency, and promote access to justice for all, but they are not a substitute for human judgment or the exercise of judicial discretion. Ensuring that AI serves as an aid rather than a replacement preserves the integrity, fairness, and legitimacy of judicial processes;

2. Judges must be willing to learn, adapt to, and appropriately embrace technological developments**,** particularly AI tools used within the legal sector, such as AI-assisted legal research platforms, case management and analytics systems, automated transcription tools, and decision-support applications**.** Equally important is an understanding of how these tools operate, including their data sources, underlying logic, capabilities, and limitations. Such knowledge enables Judges to assess the reliability of AI-generated outputs, identify potential bias or error, and exercise informed judicial oversight;

3. Judges should exercise meaningful human oversight and undertake independent verification of sources when engaging with AI-generated outputs before such information is incorporated into judicial reasoning. Reliance on unverified AI outputs risks error, bias, and misinformation, and may undermine the fairness and integrity of judicial decision-making. Independent verification ensures that AI functions as a supportive tool rather than a determinative factor in legal outcomes, thereby preserving judicial responsibility and accountability;

4. The Judiciary should initiate the enactment of a comprehensive Regulatory Framework for AI by collaborating with key stakeholders, including Parliament, the Law Society, and academic institutions, as such a framework, comprising an AI Act, regulations, and policy guidelines, will have nationwide application and promote consistency, predictability, and uniformity in the use of AI tools within the legal sector. Collaborative development ensures that the framework benefits from legislative authority, professional expertise, and scholarly insight, while also safeguarding constitutional values, judicial independence, and public trust in the administration of justice; and

5. Lastly, the Judiciary should engage in International Judicial Cooperation to share experiences, develop and adopt international best practices**,** and learn from comparative approaches to the regulation and use of artificial intelligence in the justice sector. Such collaboration facilitates the exchange of knowledge on ethical standards, governance models, risk mitigation strategies, and effective oversight mechanisms, while promoting consistency with emerging

global norms. Engaging in international judicial cooperation also enables the Judiciary to anticipate technological developments, address cross-border challenges, and strengthen public confidence in the responsible use of AI in the administration of justice. For instance, Hong Kong has the "*Guidelines on the Use of Generative Artificial Intelligence for Judges and Judicial Officers and Support Staff of the Hong Kong Judiciary*".

THANK YOU FOR YOUR KIND ATTENTION