



Law Commission of Ontario

AI IN CRIMINAL JUSTICE PROJECT

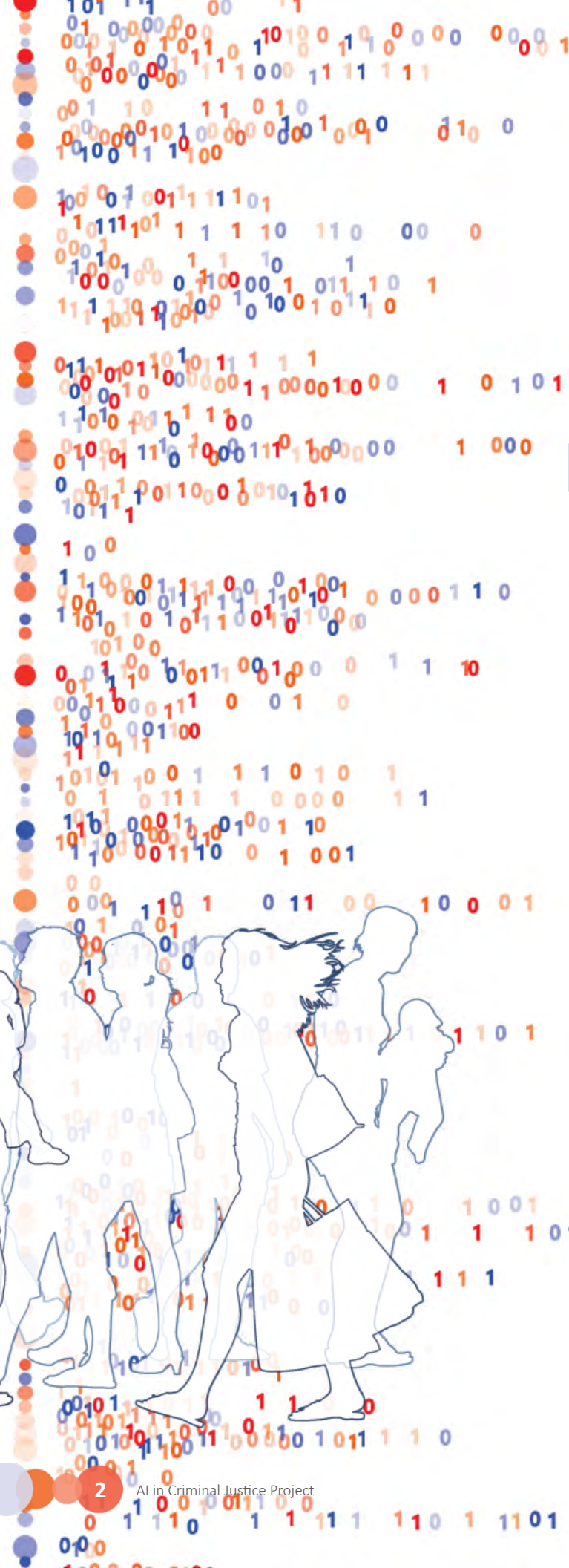
Recommendations

October 2026



Law Commission of
Ontario

Commission du droit
de l'Ontario



About The Law Commission of Ontario

The Law Commission of Ontario (LCO) is Ontario's leading law reform agency. The LCO provides independent, balanced, and authoritative advice on complex and important legal policy issues. Through this work, the LCO promotes access to justice, evidence-based legislation and policies, and public engagement on important law reform issues.

A Board of Governors, representing a broad cross-section of leaders within Ontario's justice community, guides the LCO's work. Financial support is provided by the Law Foundation of Ontario, the Law Society of Ontario, and Osgoode Hall Law School.

More information about the LCO and this project is available at: <https://lco-cdo.org>.



Law Commission of
Ontario

Commission du droit
de l'Ontario

Authors

Ryan Fritsch, Counsel, Law Commission of Ontario
Nye Thomas, Executive Director, Law Commission of Ontario

Disclaimer

The analysis and recommendations in this paper do not necessarily represent the views of the LCO's funders, supporters, Advisory Committee members or Issue Paper authors.

Project Lead and Contact

The LCO's Criminal AI Project Lead is Ryan Fritsch. He can be contacted at rfritsch@lco-cdo.org. The LCO can be contacted at:

Law Commission of Ontario
2030 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, ON, M3J 1P3

Tel: (416) 650-8406

E-mail: LawCommission@lco-cdo.org

Web: <https://lco-cdo.org>

LinkedIn: <https://linkedin.com/company/lco-cdo>

Bluesky: [@lco-cdo.bsky.social](https://bsky.social/@lco-cdo)

Funders

The LCO is funded by the Law Foundation of Ontario, Law Society of Ontario, and Osgoode Hall Law School. The LCO gratefully acknowledges the funding from the Law Commission of Canada in support of the Vancouver and Toronto roundtable consultation events.



Law Commission of Canada
Commission du droit du Canada

The AI in Criminal Justice Project

The LCO's [AI in Criminal Justice Project](#) is the first comprehensive survey and analysis of the opportunities, risks and law reform issues of AI in the Canadian criminal justice system.

In April 2025, the LCO released a project introduction and four Issue Papers. Each Issue Paper considered AI in a distinct phase of the criminal justice process:

- [Paper 1: Introduction and Summary](#)
- [Paper 2: Use of AI by Law Enforcement](#)
- [Paper 3: AI and the Assessment of Risk in Bail, Sentencing, and Recidivism](#)
- [Paper 4: AI at Trial and on Appeal](#)
- [Paper 5: AI and Systemic Oversight Mechanisms](#)

Together, the Papers presented a “lifecycle” analysis of AI throughout the Canadian criminal justice.

In addition to the project Issue Papers, the LCO convened two half-day roundtable events to consider key criminal justice AI issues, including a June 2025 [Vancouver Roundtable on the Use of Facial Recognition Technology by Law Enforcement](#) and an August 2025 [Toronto Roundtable on AI Evidence in Criminal Justice](#).

[Project Advisory Committee members](#) and [Issue Paper authors](#) include representatives from governments, police services, Crowns, the criminal defence bar, legal aid, courts administration, human rights and privacy commissions, civil society and public interest organizations, and academics.

The project included extensive consultations and engagements across the provincial and Canadian criminal justice system. In total, more than 1,400 people participated in more than public 30 discussions, workshops, conferences and public lectures across Canada.

The LCO also benefitted from a strong research and consultation partnership with the [UBC Artificial Intelligence and Criminal Justice Initiative](#), led by Professor Benjamin Perrin of the Peter A. Allard School of Law, University of British Columbia.

All project materials are available on the LCO's AI in Criminal Justice [webpage](#).



Recommendations 1-3

A Provincial Criminal Justice AI Framework

Overview

Recommendations 1-3 establish an overarching “responsible AI” framework for Ontario’s criminal justice system. This framework will ensure the use of AI systems in criminal justice promote public safety, protect legal rights and build public trust.

LCO Recommendations

1. The Province of Ontario should commit to developing a comprehensive governance framework for AI systems used in the criminal justice system in Ontario.
2. This framework should establish clear legal and policy guidance to governments, law enforcement agencies, courts, Crowns, defence counsel, legal aid and others to promote the responsible development and deployment of AI in Ontario’s criminal justice sector.
3. The key elements of this framework should include:
 - a. Mandatory, public disclosure of AI systems in criminal justice.
 - b. Risk criteria identifying prohibited, high-risk, restricted use and low-risk uses of AI systems in criminal justice.
 - c. A dedicated and mandatory impact assessment for AI systems in criminal justice.
 - d. A duty to evaluate AI systems in criminal justice for reliability, validity, bias, and conformity with the *Charter*, human rights law, privacy law, and criminal procedural and evidentiary requirements, and for law enforcement services to additionally evaluate lawful authority and purpose.
 - e. Procedural protections, such as warrant requirements for high-risk systems and dedicated rules governing AI-generated or enhanced evidence in different proceedings.
 - f. Support for criminal justice AI pilots.
 - g. Mandatory and ongoing auditing and evaluation requirements.
 - h. Procurement standards and policies governing responsible software practices including software explainability, version control and archiving, training data disclosure and transparency, and reports on reliability, validity and bias of the system.
 - i. An independent supervisory body to support oversight of individual AI systems and provincial AI systems in criminal justice generally.
 - j. Guarantees for judicial independence and investigative privilege for law enforcement.
 - k. Commitments that will ensure access to justice and equitable access to AI legal tools.



Recommendations 4-9

Provincial Criminal Justice AI Legislation

Overview

LCO Recommendations 4-9 set out the key AI governance requirements that should be included in provincial legislation. Legislation will establish a comprehensive, consistent baseline for AI systems in criminal justice.

LCO Recommendations

4. The Government of Ontario should amend the [*Enhancing Digital Security and Trust Act, 2024*](#), or create complementary legislation, to enshrine significant governance principles and requirements in provincial legislation for AI systems in criminal justice. This legislation (or accompanying regulations) should:
 - a. Include a preamble specifying that AI systems in criminal justice are subject to a precautionary principle, and must comply with the *Charter*, principles of criminal procedural fairness, privacy law, human rights law, criminal common law, and the principle of judicial independence.
 - b. Establish mandatory risk categories for AI systems in criminal justice, including:
 - i. Prohibited systems.
 - ii. High-risk systems.
 - iii. Restricted use systems.
 - iv. Low-risk systems.
 - c. Require AI systems in criminal justice to:
 - i. Be disclosed on a public AI registry.
 - ii. Be subject to a dedicated and mandatory impact assessment.
 - iii. Comply with procedural and evidence standards.
 - iv. Be audited and evaluated on an ongoing basis.
5. The legislation should establish reporting requirements to Ontario's Inspector General of Policing and Law Enforcement Complaints Agency, who will provide an annual public report analyzing the use of AI by law enforcement services (see also Recommendations 19-20).
6. The legislation should establish the authority to create a dedicated provincial supervisory authority for AI systems in criminal justice (see also Recommendations 19-20).
7. The legislation should require law enforcement services to establish dedicated AI operational and governance policies and designate officials responsible for the policy's implementation.
8. The legislation should require digital sovereignty over high-risk and restricted use AI systems in criminal justice and regulate standard terms for vendor contracts necessary to fulfil all mandated assessment, disclosure and other obligations.
9. The legislation should mandate several public engagement measures including public participation in AI assessment, annual reporting requirements, a role for the public in the dedicated provincial supervisory authority, and legislative reviews every two years.



Recommendations 10-15

Criminal AI Risk Management

Overview

LCO Recommendations 10-15 establish a comprehensive risk management framework to govern AI systems in Ontario's criminal justice system. The recommendations identify risk categories (Prohibited, High Risk, Restricted Use and Low Risk), use cases and mitigation measures. The Recommendations match governance obligations to an AI system's uses, benefits and risks; promote responsible AI adoption; build public trust; and uphold the principles and requirements of Canadian law.

LCO Recommendations

10. The legislative framework described in Recommendation 4 should prescribe four risk categories for criminal justice AI systems used in Ontario, including “prohibited”, “high-risk”, “restricted use” and “low-risk” systems.
11. The provincial government should conduct public consultations to identify the risk criteria, contexts and uses of AI systems, including but not limited to systems that may be prohibited, pre-emptively identified as high-risk, or otherwise subject to higher regulatory standards.

Prohibited AI Systems

12. Prohibited AI systems in criminal justice could include the following:

- a. Prohibited Risk Criteria
 - i. Prohibited AI systems are those posing unacceptable risks to fundamental rights and Canadian values.
 - ii. Unacceptable risks may include uses for AI that are particularly harmful and that contradict Canadian values of respect for fundamental rights under the *Charter* (including fundamental freedoms, democratic rights, mobility rights, civil liberties, equality and the rule of law), rights established in federal and provincial human rights codes (including inherent dignity, equality, and protection from discrimination and harassment), privacy rights, and procedural fairness.
- b. Prohibited AI Practices
 - i. Real-time remote biometric surveillance, including direct identification of individuals (facial recognition) or object detection for the purpose of inferring identity (object tracking, gait analysis, etc.).
 - ii. Individual criminal offence risk assessment and prediction, including assessing eligibility and conditions for bail.
 - iii. Social scoring to evaluate or classify natural persons or groups of persons based on social behaviour or personal or personality characteristics, with the social score leading to detrimental or unfavourable treatment.
 - iv. Emotion recognition.
 - v. Biometric categorization based on biometric data to deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, or sexual orientation.
 - vi. Predictive systems to forecast the likelihood that a person will commit a criminal offense or the predicted location of criminal activity.
 - vii. Agentic AI systems, other than for backend administrative purposes deemed low risk.
 - viii. Adjudication of criminal cases and conduct investigations of criminal justice professionals.

High-Risk AI Systems

13. High-risk AI systems in criminal justice could include the following:

- a. Criteria for Determining High Risk
 - i. High-risk AI systems are those posing a reasonably foreseeable risk of harm to fundamental rights under the *Charter* (including fundamental freedoms, democratic rights, mobility rights, civil liberties, equality and the rule of law), rights established in federal and provincial human rights codes (including inherent dignity, equality, and protection from discrimination and harassment), privacy rights, or procedural fairness.
 - ii. Reasonably foreseeable risks include but are not limited to: systems that materially influence the outcome of a decision or have a differential impact on vulnerable groups.
- b. High-Risk AI Practices
 - i. Biometric identification.
 - ii. Object identification and tracking systems, such as license plate readers.
 - iii. Surveillance, including the collection, use and analysis of personal information or online “open-source” publicly available personal information, and surveillance on the basis of personal characteristics and behaviour such as location and movement, speech, features, and physical interactions amongst groups and/or individuals.
 - iv. Forensic analysis, including analyzing both digital and physical evidence as it relates to investigating a specific criminal incident.
 - v. AI-generated description, summary or transcription of speech and events, and the generation or editing of incidence/occurrence reports.
 - vi. Production of any forms of AI evidence that may be relied on in proceedings with lower evidentiary burden including bail hearings, diversion hearings, and applications for judicial authorization.
 - vii. Cross-linking, comparing, comingling or otherwise subjecting different databases to AI analysis, including voluntary third party disclosures.
- c. Mitigation
 - i. Risk-based regulations should tailor legal obligations proportionately so that the most onerous obligations only attach to the highest-risk systems. Risks associated with High-Risk AI Systems could be mitigated by measures including, but not limited to:
 - Rights impact assessment and assessment of lawful purpose and scope of use.
 - Procurement standards.
 - A requirement to only use previously assessed and authorized AI software and devices in the scope of any professional duty.
 - Procedural protections including human-in-the-loop certification of outputs and ongoing labeling of AI throughout the chain of evidence.
 - AI compliance by design including audit trails for prompts and alterations.
 - Adequate technical and performance assessment for reliability, validity and bias tested in real-world conditions.
 - Ongoing documentation, transparency, reporting, oversight and quality management systems.

Restricted-Use AI Systems

14. Restricted-use AI systems in criminal justice could include the following:

a. Restricted-Use Risk Criteria

- i. Restricted-Use AI systems are those posing risks of adverse impacts on individuals or society, harm to the administration of justice; or which may undermine public confidence in the criminal justice system.

b. Restricted-Use AI Practices

- i. Front-end support tools that aid in non-investigatory interactions with the public. Examples include (but are not limited to):
 - Voice recognition or chatbot systems that provide an intake, triage, or informational function.
 - Translation and transcription, including post-facto and real-time services.
 - Generating or altering audio, image, video or text content.
 - AI queries for legal or policy information or guidance shared or acted on in the course of professional duties to the public.
- ii. Use of AI by judges, crowns, and defence to analyze or prepare legal materials or submissions including evidentiary analysis, disclosure, facta and submissions as an aid to drafting judgments, and other material.

c. Mitigation

- i. Risk-based regulations should tailor legal obligations proportionately so that the most onerous obligations only attach to the highest-risk systems. Risks associated with Restricted-Use AI systems could be mitigated by measures including, but not limited to:
 - Rights impact assessment and assessment of lawful purpose and scope of use.
 - Procurement standards.
 - A requirement to only use previously-assessed and authorized AI software and devices in professional duties.
 - Procedural protections including human-in-the-loop certification of outputs and ongoing labeling throughout the chain of evidence.
 - AI compliance by design, including audit trails for prompts and alterations.
 - Adequate technical and performance assessment for reliability, validity and bias tested in real-world conditions.
 - Ongoing documentation, transparency, reporting, oversight and quality management systems.
 - Ongoing professional training and enforcement related to the weaknesses and responsible use of AI systems.
 - Notice to the public about the use of an AI system.

Low-Risk AI Systems

15. Low-Risk Uses of AI in Ontario's criminal justice system should consider incorporating the following:

- a. Criteria for Determining Low Risk
 - i. Low Risk AI systems are those that do not pose any risk of harm to fundamental rights, risk of adverse impacts on individuals or society, harm to the administration of justice, and which do not undermine public confidence in the criminal justice system.
 - ii. Low-Risk AI systems include AI systems which perform a narrow procedural or preparatory task, do not materially influence or replace the outcome of an assessment or decision-making, and are easily corrigible or reversible.
- b. Low-Risk AI Practices
 - i. Backend administrative systems that may aid in routine internal functions or management operations, reducing time or labor, gaining efficiencies or training.
 - ii. AI systems that perform an assistive function for standard editing or do not materially alter the input data provided by the user.
 - iii. Use of AI-enabled security tools for the purpose of data security within criminal justice organizations.



Recommendations 16-18

Public AI Registry, Standard AI Assessment, and Digital Sovereignty and Procurement

Overview

LCO Recommendations 16-18 provide additional directions on key legislative or regulatory provisions, including a public AI registry, risk assessments, digital sovereignty and procurement.

LCO Recommendations

16. Provincial legislation should require mandatory disclosure of AI systems in criminal justice, including posting of key details about the system on a public registry.
 - a. Public disclosures should include key information about the purpose, general capabilities, risk categorization, mitigation strategies, and relevant impact assessments about the AI systems.
 - b. Public disclosure reports should account for the independence of the judiciary and investigative privilege for law enforcement.
 - c. Public disclosures should be updated upon a material change in the capabilities, purpose or use of the system or annually, whichever comes first.
17. The Government of Ontario should work with relevant stakeholders to develop a dedicated and mandatory impact assessment for AI systems in criminal justice. The impact assessment should assess the AI system for:
 - a. Compliance with the *Charter*, principles of criminal procedural fairness, criminal common law precedents, human rights law, and privacy law.
 - b. Lawful authority and lawful purpose.
 - c. Evidentiary admissibility.
 - d. Bias.
 - e. Other technical, safety, and assurance factors.
18. Additional legislative or regulatory provisions should include:
 - a. Explicit authorization of pilots to evaluate the use, effectiveness, legality, and cost-benefit of AI systems in criminal justice in real-world conditions.
 - b. Dedicated procurement standards and regulations governing responsible software practices including software explainability, version control and archiving, training data disclosure and transparency, and the provision of reports assessing the reliability, validity and bias of the system.
 - c. Requirements to protect digital sovereignty in AI systems in criminal justice, including requirements that the collection, use, processing, transmission and storage of information associated with high-risk and restricted-use systems and data occurs within Canada, and by regulating standard terms for vendor contracts necessary to fulfil all mandated assessment, disclosure and other obligations.



Recommendations 19-20

Oversight and Reporting

Overview

LCO Recommendations 19-20 establish oversight and reporting obligations. These recommendations commit the province to establishing a dedicated supervisory body for AI systems in criminal justice. In the interim, the recommendations add reporting, oversight and advisory functions to Ontario's Inspector General of Policing, Law Enforcement Complaints Agency, and others.

LCO Recommendations

19. The Province of Ontario should create an independent supervisory body for AI systems used in the provincial criminal justice system. This body should be established in provincial legislation. This body's mandate should include:
 - a. AI assessment, certification, and ongoing evaluation.
 - b. Creation of a multi-disciplinary public advisory board and technical work groups.
 - c. Availability of expert opinions and witnesses.
 - d. Maintaining a provincial registry of AI systems in criminal justice including publication of associated mandatory AI assessment reports.
 - e. Enforcement of related standards and duties.
20. Pending establishment of the supervisory body, the Province of Ontario should enact interim legislation, regulations, or rules and policies to ensure existing institutions can fulfil oversight roles for AI systems in criminal justice, including:
 - a. Requiring that Ontario's Inspector General of Policing and Ontario's Law Enforcement Complaints Agency receive yearly reports from law enforcement agencies with a comprehensive inventory of criminal justice AI systems, risk assessments, and AI governance and operational policies.
 - b. Requiring that Ontario's Inspector General of Policing and Ontario's Law Enforcement Complaints Agency publish an annual public report analyzing the use of AI by law enforcement services and any regulatory actions taken, including development of model AI governance and operational policies for law enforcement.
 - c. Establishing a Crown Criminal AI Advisory Office within the Minister of the Attorney General to provide advice to law enforcement on the investigative uses of AI and to inform AI assessments.



Recommendations 21-24

AI Evidence

Overview

LCO Recommendations 21-24 address AI-created or AI-enhanced evidence that might be used in criminal proceeding or during a criminal investigation. These recommendations account for the shared jurisdiction in these matters between the provincial government, federal government and various Rules committees, and the need to develop dedicated evidentiary rules for different stages of the criminal justice process.

LCO Recommendations

21. The Province of Ontario should encourage the federal government to convene a joint Federal-Provincial Criminal AI Evidence Rules Committee and consultation process. The mandate of this committee should be comparable to that of the Artificial Intelligence Subcommittee of the Civil Rules Committee to study and recommend a set of minimum safeguards for AI evidence rules for criminal matters.
22. The Courts of Criminal Justice in Ontario should use powers delegated under the *Courts of Justice Act* and the *Criminal Code* to convene a Criminal Proceedings Rules AI Evidence Subcommittee. The mandate of the committee should be comparable to that of the Ontario Civil Rules Committee AI Subcommittee to study and recommend a set of AI evidence rules for different provincial criminal proceedings.
23. The Ontario Ministry of the Attorney General” should establish an AI Evidence Policy and Procedure Committee. The mandate of the committee should be to study, consult on, and draft a set of AI evidence procedural policies for different provincial criminal proceedings. In particular, policies should:
 - a. Confirm the prohibition on the use of AI tools for the purpose of assessing risk, and the high risk designation of AI evidence in bail proceedings, consistent with LCO Recommendations 12.b.ii and 13.b.vi.
 - b. Establish a disclosure and certification process for any forms of AI evidence that may be considered in a bail proceeding.
24. The Ontario Ministry of the Attorney General should amend the Crown Prosecution Manual with policy directives implementing the recommendations developed above.



Recommendations 25-29

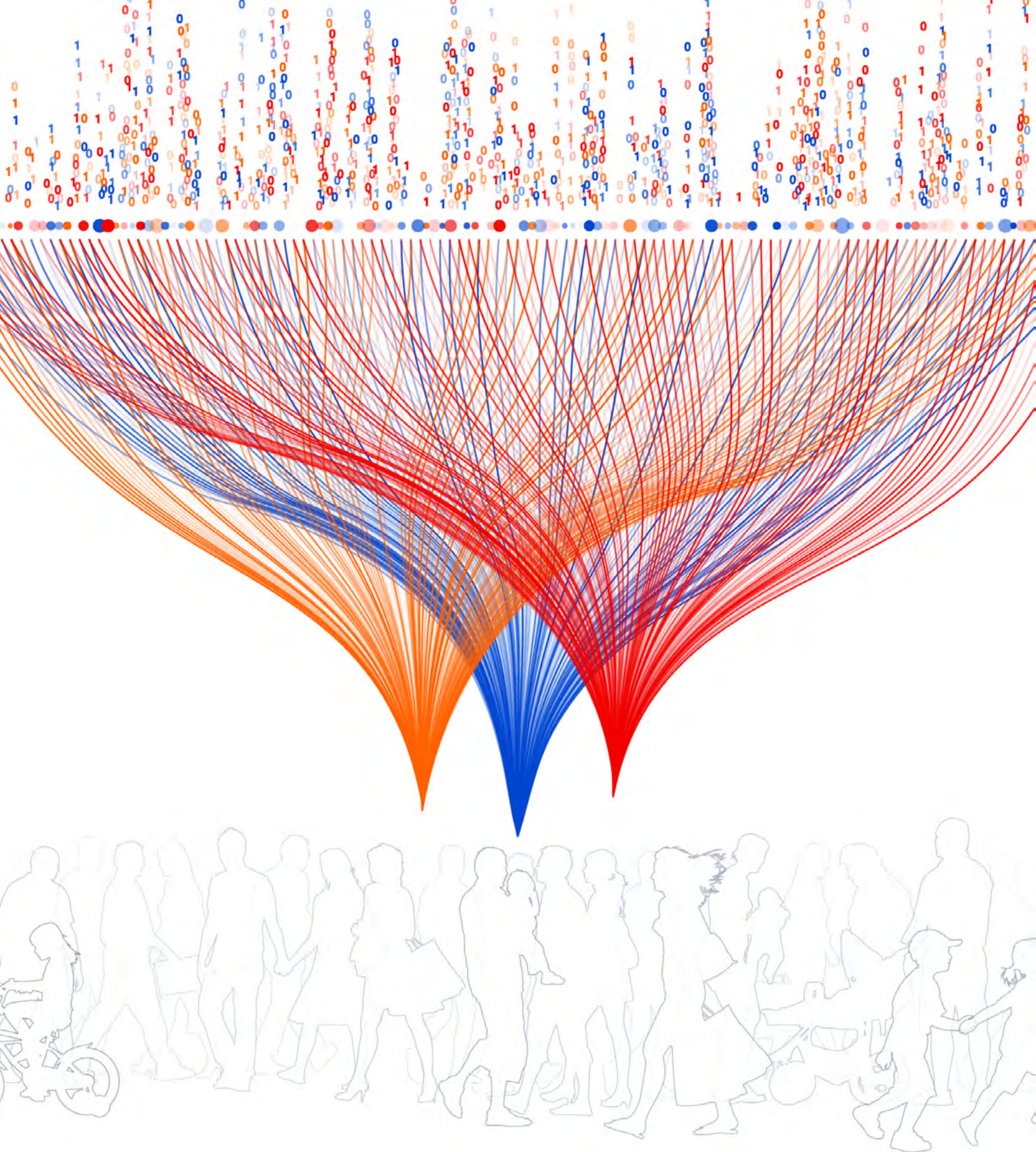
Access to Justice and System Capacity

Overview

Recommendations 25-29 address the need to ensure criminal accused and defence counsel have meaningful access to justice in criminal proceedings involving AI systems. These recommendations also address the need to increase capacity within provincial criminal justice institutions to effectively respond to the foreseeable challenges of AI systems.

LCO Recommendations

25. The provincial Ministry of the Attorney General should increase funding and other resources for Legal Aid Ontario as necessary to ensure criminal defence counsel are able to make a full answer and defence in cases involving AI evidence.
26. Legal Aid Ontario should establish an AI Centre of Excellence with the mandate and resources to support staff and private bar defence counsel, duty counsel, and legal aid clinics with:
 - a. Comprehensive training on criminal justice AI-related laws and procedures.
 - b. Standards for professional competence in AI legal research and advocacy.
 - c. Legal research on AI issues and cases.
 - d. Support for individual and systemic AI test cases.
27. Legal Aid Ontario should establish an external advisory committee with a mandate to meet regularly and advise LAO's board and management on the purpose, design, implementation and foreseeable impacts of any proposed criminal justice-related AI systems, programs, procedures or services.
28. Pending establishment of the supervisory authority for AI in criminal justice recommended above, the Centre of Forensic Sciences should develop a program freely available to criminal defence counsel who seek an opinion on the reliability, validity and bias of AI evidence, investigation tools, and investigation practices. This program could include a roster of independent AI experts available to the defence.
29. Pending establishment of the supervisory authority for AI in criminal justice recommended above, the Centre of Forensic Sciences should develop a program for the certification and provision of AI-related forensic tools to legal counsel, such as platforms for identifying deepfake evidence and documents.



Law Commission of
Ontario
Commission du droit
de l'Ontario

2030 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, Ontario, Canada M3J 1P3