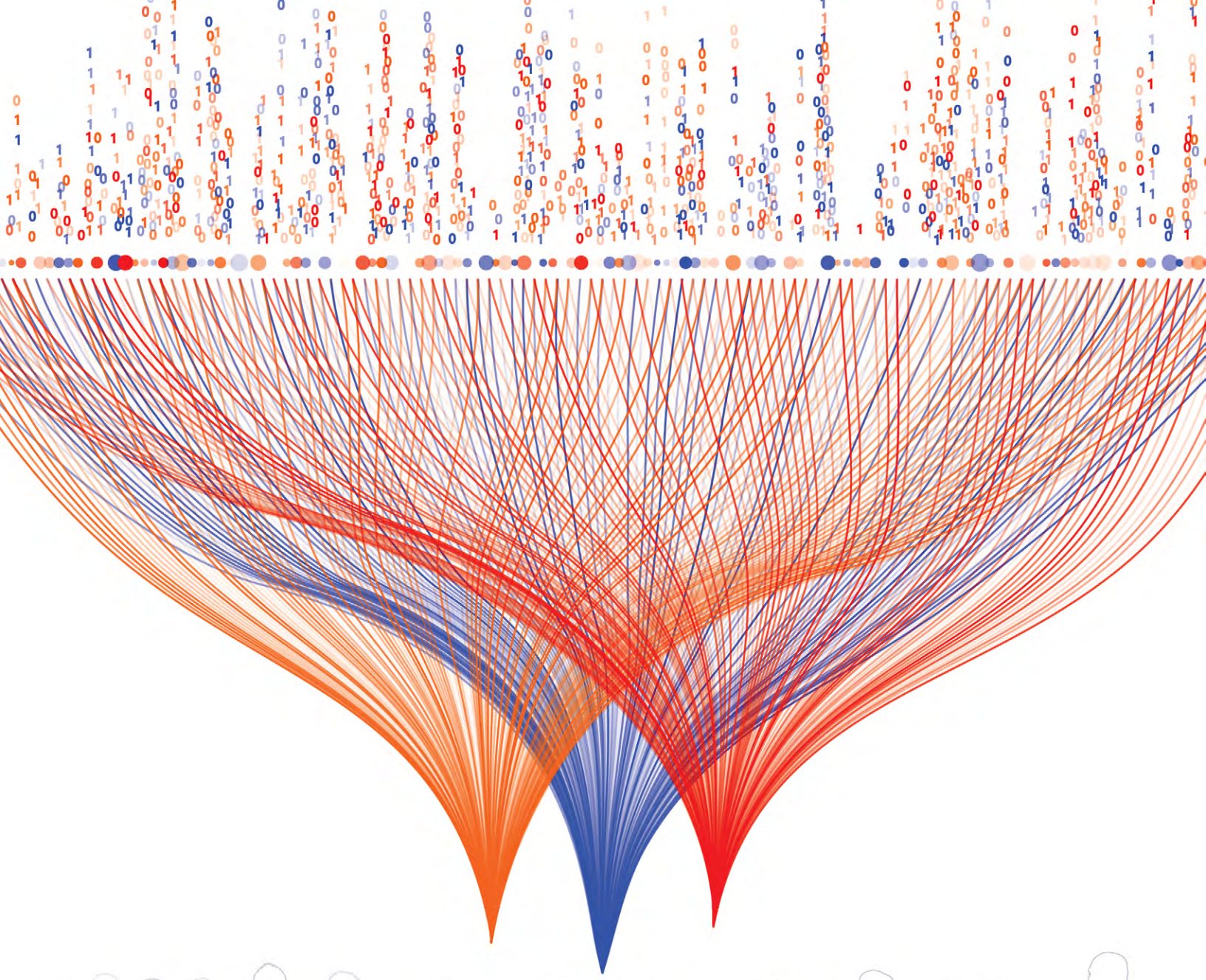


Commission du droit de l'Ontario

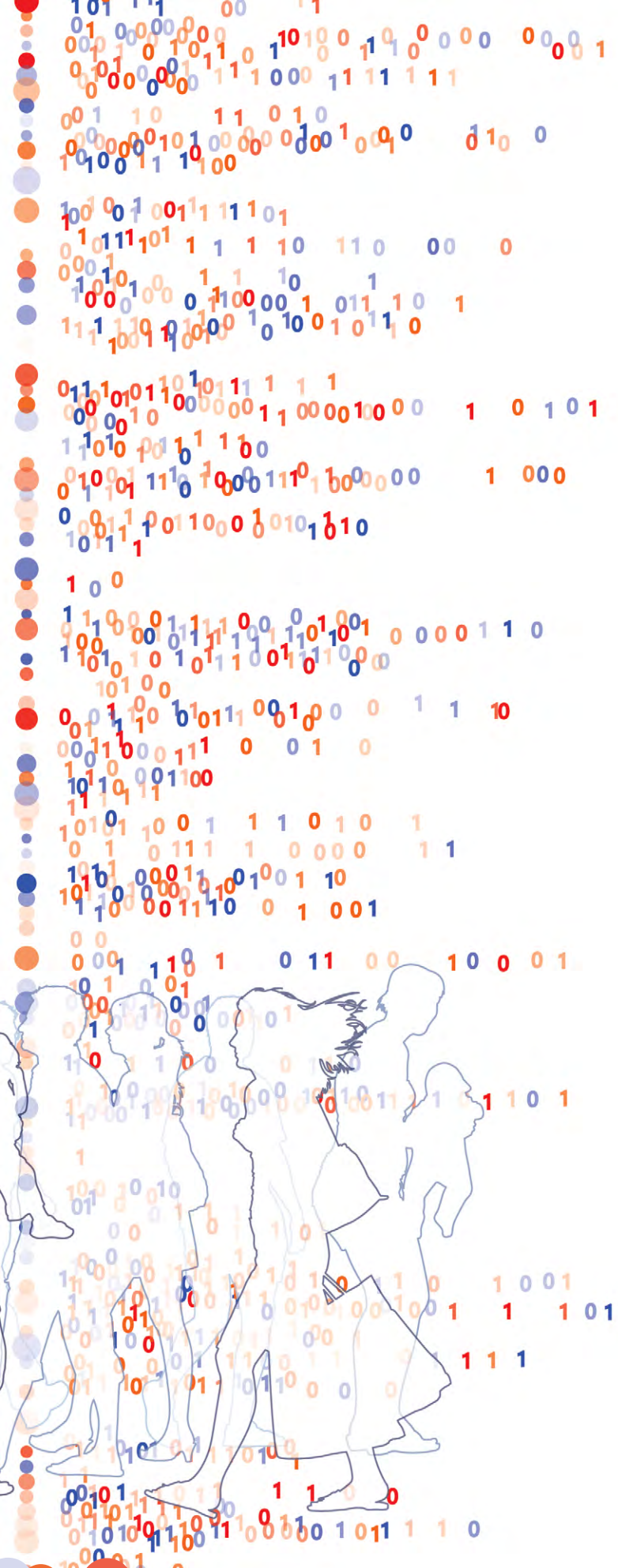
PROJET SUR L'IA DANS LE SYSTÈME DE JUSTICE PÉNALE | ANNEXE A

# Sommaire et questions de consultation

Avril 2025

LCO
CDO

LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO



## À propos de la Commission du droit de l'Ontario

La Commission du droit de l'Ontario (CDO) est un organisme de premier plan en matière de réforme du droit en Ontario.

La CDO fournit des avis indépendants, équilibrés et faisant autorité sur des questions juridiques complexes et importantes. Grâce à ce travail, la CDO favorise l'accès à la justice, l'élaboration de lois et de politiques fondées sur des données probantes, ainsi que la participation du public à d'importantes questions de réforme législative. La CDO est indépendante des intérêts des parties prenantes et s'engage à adopter une perspective d'intérêt public dans tous ses projets.

Voici des rapports et mémoires récents de la CDO traitant des questions liées à l'IA :

- Évaluation de l'impact de l'intelligence artificielle sur les droits de la personne (avec la Commission ontarienne des droits de la personne, 2024)
- Mémoire au gouvernement de l'Ontario sur le projet de loi 194 (2024)
- *Accountable AI* (2022)
- *Réglementer l'intelligence artificielle – Enjeux et choix essentiels* (2021)
- *Legal Issues and Government AI Development* (2021)
- The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada (2020)

Pour en savoir plus sur la CDO et ce projet, veuillez consulter : https://www.lco-cdo.org/fr.

## Source

Commission du droit de l'Ontario
2032, édifice Ignat Kaneff
Faculté de droit Osgoode Hall, Université York
4700, rue Keele, Toronto ON M3J 1P3

Tél. : 416 650-8406
Courriel : LawCommission@lco-cdo.org
Web : https://www.lco-cdo.org
LinkedIn : https://linkedin.com/company/lco-cdo
Bluesky : @lco-cdo.bsky.social
X : @LCO_CDO
YouTube : @lawcommissionofontario8724

## Bailleurs de fonds

la Commission du droit de l'Ontario est financée par la Fondation du droit de l'Ontario, le Barreau de l'Ontario et la faculté de droit Osgoode Hall. La CDO est située à la faculté de droit Osgoode Hall à Toronto.

## Projet de la CDO sur l'IA dans le système de justice pénale

Rapport 1 Introduction et sommaire : projet sur l'IA dans le système de justice pénale :
Nye Thomas, directeur général, CDO
Ryan Fritsch, avocat, CDO

Rapport 2 L'utilisation de l'IA par les forces de l'ordre
Ryan Fritsch, avocat, CDO

Rapport 3 L'IA et l'évaluation du risque associé à la mise en liberté sous caution, à la détermination des peines et à la récidive
Armando D'Andrea, avocat-conseil, bureau provincial, Aide juridique Ontario
Gideon Christian, professeur de droit, faculté de droit, Université de Calgary

Rapport 4 L'IA durant le procès et en appel
Paula Thompson, Initiatives stratégiques, ministère du Procureur général
Eric Neubauer, avocat de la défense, Neubauer Law, et coprésident, Criminal Lawyers Association Technology Committee

Rapport 5 L'IA et les mécanismes de surveillance systémique dans le système de justice pénale
Brenda McPhail, conseillère principale en technologie et en politiques, Commissaire à l'information et à la protection de la vie privée de l'Ontario
Marcus Pratt, conseiller principal, Service des politiques, Aide juridique Ontario et président du comité des causes types d'AJO
Jagtaran Singh, conseiller juridique, Commission ontarienne des droits de la personne

Annexe A Sommaire et liste des questions de consultation

Annexe B Études de cas du projet

Vous pouvez consulter les documents en ligne au : www.lco-cdo.org/fr/nos-projets-en-cours/lia-dans-le-systeme-de-justice-penale

## Rédacteurs en chef

**Nye Thomas**, directeur général, CDO
**Ryan Fritsch**, avocat, CDO

## Chercheurs étudiants

Thurka Brabaharan
Dixon Emanuel
Nouran Hamzeh
Shahmurad Lodhi
Masha Michouris
John Nyman
Ani Semanjaku

## Comité consultatif externe

**Alpha Chan**, responsable de la sécurité de l'information, Service de police de Toronto

**Marco Galluzzo**, cabinet du juge en chef, Cour supérieure de justice de l'Ontario

**Rosanna Giancristiano**, directrice des opérations judiciaires, ministère du Procureur général

**Rosemarie Juginovic**, cabinet du juge en chef, Cour supérieure de justice de l'Ontario

**Professeur agrégé Daniel Konikoff**, département de sociologie, Université de l'Alberta

**Michelina Longo**, directrice des relations extérieures, ministère du Solliciteur général

**Jessica Mahon**, Section des normes policières, ministère du Solliciteur général

**Jane Mallen**, ministère du Procureur général et Conseil des gouverneurs de la CDO

**Elena Middelkamp**, Bureau des avocats de la Couronne- droit pénal, ministère du Procureur général

**Savio Pereira**, Section des normes policières, ministère du Solliciteur général

**Professeur Ben Perrin**, faculté de droit, Université de la Colombie-Britannique

**Michael Swinburne**, conseiller principal en politiques, Commission canadienne des droits de la personne

**Professeur David Murakami Wood**, département de criminologie, Université d'Ottawa

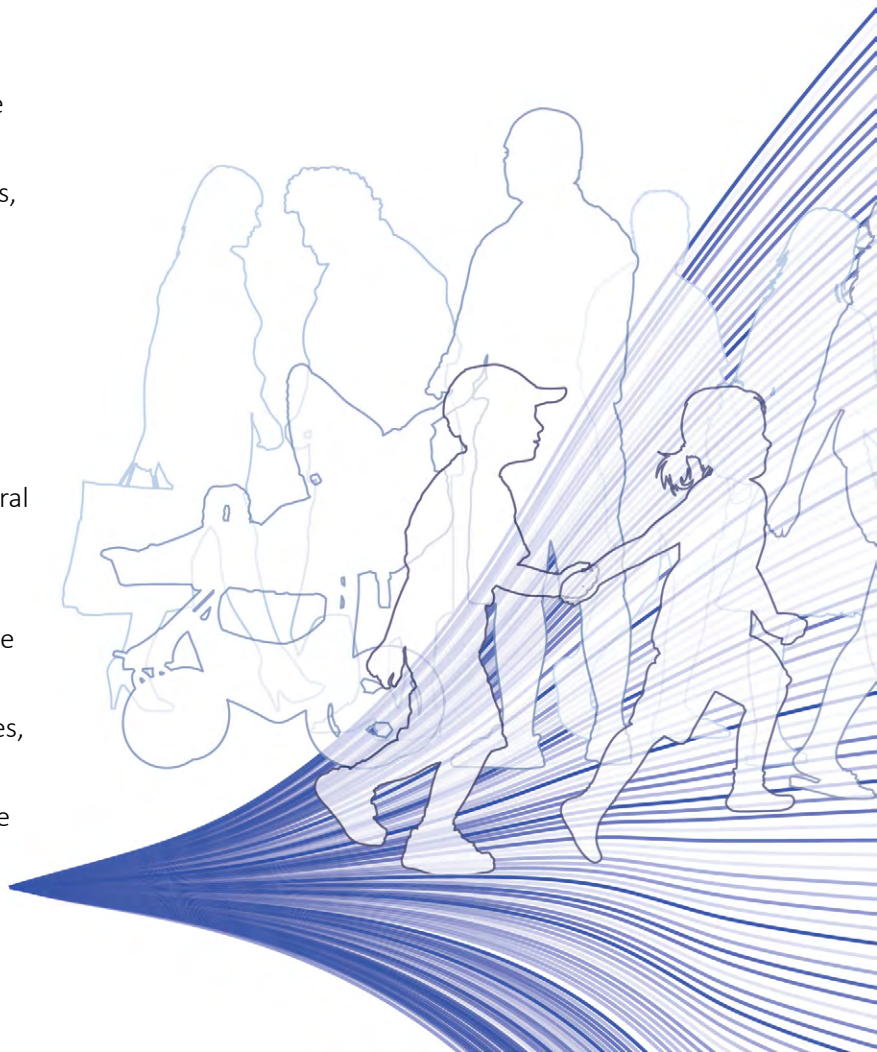
## Non-responsabilité

l'analyse, les conclusions et les recommandations présentées dans le présent document ne reflètent pas nécessairement les opinions des bailleurs de fonds, des contributeurs, des membres du comité consultatif ou des auteurs des documents thématiques de la CDO.

L'analyse, les conclusions et les recommandations présentées dans les documents thématiques du projet ne reflètent pas nécessairement les opinions de la CDO, de ses bailleurs de fonds, de ses contributeurs ou des membres du comité consultatif.

## Référence

commission du droit de l'Ontario, *Sommaire et liste des questions de consultation : projet sur l'IA dans le système de justice pénale* (avril 2025).



# Table des matières

# 1. Projet de la CDO sur l'IA dans le système de justice pénale

Le projet sur l'IA dans le système de justice pénale de la Commission du droit de l'Ontario (CDO) est une étude et une analyse novatrices sur l'intelligence artificielle (IA) dans le système de justice pénale canadien.

Ce projet est le fruit d'une collaboration unique entre des praticiens et des experts de premier plan de partout au Canada. Parmi les auteurs et les conseillers, on compte des représentants des gouvernements, des services de police, des avocats de la Couronne, des avocats de la défense, des tribunaux, des services d'aide juridique, des commissions des droits de la personne, d'organisations civiles et du milieu universitaire.

Le projet comprend une introduction et quatre documents thématiques. Chaque document thématique examine l'utilisation de l'IA dans une phase distincte du processus de justice pénale, notamment :

- L'utilisation de l'IA par les forces de l'ordre
- L'IA et l'évaluation du risque associé à la mise en liberté sous caution, à la détermination des peines et à la récidive
- L'IA durant le procès et en appel
- L'IA et les mécanismes de surveillance systémiques

Le projet s'articule autour de quatre thèmes ou sujets clés :

Tout d'abord, le projet examine les importants enjeux pratiques et juridiques auxquels font face les services de police, les tribunaux, les décideurs politiques, les procureurs de la Couronne, les avocats de la défense et les criminels accusés au Canada, notamment :

- Quels outils d'IA sont utilisés, ou pourraient être utilisés, à chaque étape du système de justice pénale canadien?
- Quels sont les avantages et les risques associés à ces technologies?
- Quels enjeux juridiques pourraient se poser à chaque étape, en particulier en ce qui concerne la *Charte des droits et libertés*, l'équité procédurale, le droit de la preuve et les principes de common law régissant le droit criminel?
- Où en sont le droit et les procédures au Canada concernant le traitement de ces enjeux, et quelles mesures proactives doivent être prises pour harmoniser les pratiques et les normes de manière systémique?

Deuxièmement, le projet cherche à déterminer qui est susceptible d'être touché par l'IA dans le système de justice pénale.

Troisièmement, le projet examine et analyse les initiatives internationales et canadiennes récentes pour mettre en place une « IA fiable dans le système de justice pénale ».

Enfin, le projet tente de prévoir ou de prédire ce qui pourrait se passer si aucune mesure n'est prise.

Les documents thématiques sur l'IA dans le système de justice pénale de la CDO sont conçus pour faciliter la discussion et la consultation. Nous avons appris que la « fiabilité de l'IA dans le système de justice pénale » repose sur des considérations juridiques, techniques et opérationnelles complexes. Nous avons également appris qu'il est essentiel de mener des collaborations et des consultations à grande échelle. Par conséquent, chaque document thématique comprend des questions destinées aux décideurs politiques et aux parties prenantes du Canada sur l'IA dans le système de justice pénale. Ces questions sont résumées à l'annexe A du présent sommaire. La CDO espère ainsi que ces documents serviront de catalyseur à un débat plus large au Canada sur ces questions importantes et d'actualité.

La publication des documents thématiques marque le début d'une période de consultation des parties prenantes menée par la CDO. La CDO analysera et résumera les commentaires reçus. Elle recommandera dans un rapport final une série de réformes législatives, politiques et programmatiques.

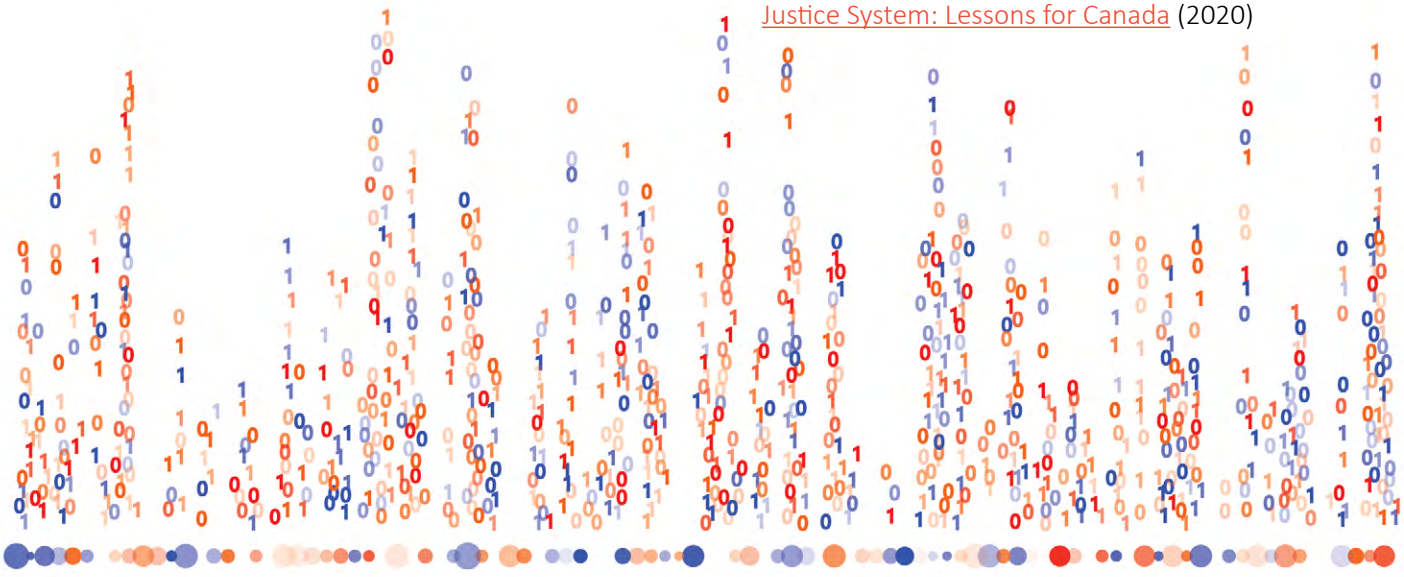
Pour en savoir plus sur ce projet, consultez le site Web des projets de la CDO : https://www.lco-cdo.org/fr/nos-projets-en-cours/lia-dans-le-systeme-de-justice-penale/.

# 2. À propos de la CDO

La Commission du droit de l'Ontario est un organisme de premier plan en matière de réforme du droit en Ontario. La CDO fournit des avis indépendants, équilibrés et faisant autorité sur des questions juridiques complexes et importantes. La CDO favorise l'accès à la justice, l'élaboration de lois et de politiques fondées sur des données probantes, ainsi que la participation du public à d'importantes questions de réforme législative. La CDO est indépendante des intérêts des parties prenantes et s'engage à adopter une perspective d'intérêt public dans tous ses projets. Vous trouverez plus de renseignements sur la CDO ici.

Ce projet est l'un des nombreux projets de la CDO traitant des questions liées à l'IA dans le système judiciaire canadien. Parmi les projets et rapports antérieurs, mentionnons :

- Évaluation de l'impact de l'intelligence artificielle sur les droits de la personne (avec la Commission ontarienne des droits de la personne, 2024)
- *Accountable AI* (2022)
- *Réglementer l'intelligence artificielle – Enjeux et choix essentiels* (2021)
- *Legal Issues and Government AI Development* (2021)
- The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada (2020)



# 3. L'IA dans le système de justice pénale : usages et avantages

Partout dans le monde, le système de justice pénale a été à l'avant-garde de l'adoption de l'IA. Des juridictions pénales à l'extérieur du Canada utilisent l'IA pour améliorer les enquêtes policières, analyser les preuves, contribuer à la prise de décisions judiciaires, optimiser l'analyse des données et cibler les ressources. Les technologies d'IA actuellement utilisées dans le système de justice pénale comprennent le maintien de l'ordre prédictif, la technologie de reconnaissance faciale (TRF) et la surveillance biométrique, l'analyse des médias sociaux, les lecteurs de plaques d'immatriculation, les algorithmes pour les libérations conditionnelles et la détermination des peines, et bien d'autres applications. Bon nombre de ces systèmes seraient également utilisés au Canada. Parmi les systèmes d'IA notables dans le secteur pénal, on peut citer :

## 1. L'analyse prédictive/le maintien de l'ordre prédictif[1]

Le maintien de l'ordre prédictif est un nom générique désignant une technologie d'IA qui traite et analyse des ensembles de données volumineux et complexes beaucoup plus rapidement que les humains. Le professeur Andrew Ferguson, éminent spécialiste américain en maintien de l'ordre prédictif, écrit que :

> *…les informations issues des données sont utilisées pour prendre des décisions concrètes concernant les priorités de la police et l'allocation des ressources… offrant ainsi aux responsables de la police la possibilité d'identifier les zones à forte criminalité, de restructurer les itinéraires de patrouille et d'élaborer des stratégies de lutte contre la criminalité basées sur les nouvelles données*[2].

Le maintien de l'ordre prédictif est généralement compris comme étant formé de systèmes d'IA qui tentent de prévoir les crimes futurs, notamment[3] :

- les systèmes géolocalisés qui prédisent où et quand des activités criminelles pourraient se produire ;
- les systèmes personnels qui prédisent qui est susceptible d'être impliqué dans des activités criminelles futures.

Parmi les exemples bien connus du maintien de l'ordre prédictif, on peut citer LASER, un système que la police de Los Angeles utilisait pour identifier les zones où des violences armées étaient susceptibles de se produire ; PredPol et Palantir, les systèmes de maintien de l'ordre prédictif les plus couramment utilisés aux États-Unis ;

et le système de « liste stratégique des personnes à surveiller » de la police de Chicago[4]. Les services de police canadiens auraient également utilisé ou testé le maintien de l'ordre prédictif, notamment le service de police de Vancouver (GeoDASH) et le service de police de Calgary (Palantir Gotham)[5].

## 2. Reconnaissance faciale et biométrie[6]

La Commissaire à l'information et à la protection de la vie privée de l'Ontario définit la technologie de reconnaissance faciale (TRF) comme suit :

> *… une technologie de l'intelligence artificielle (IA) qui permet de recueillir et de traiter des renseignements personnels délicats pour identifier un particulier ou vérifier son identité… Le système de reconnaissance faciale peut alors comparer deux empreintes faciales et produire une cote de similarité ou jumeler des empreintes faciales à l'issue d'une recherche dans une base de données de référence contenant un grand nombre d'images pour obtenir une liste de candidats possibles, dont la cote de similarité est égale ou supérieure à un seuil établi*[7].

Outre la TRF, d'autres formes d'identification biométrique optimisées par l'IA comprennent les empreintes digitales, la reconnaissance vocale, la reconnaissance de l'iris et l'analyse de la démarche.

De nombreux services policiers estiment que la TRF et d'autres technologies biométriques présentent un potentiel considérable pour améliorer la sécurité publique, les enquêtes policières et le rendement. Par exemple, INTERPOL a déclaré que :

> *…la vision par ordinateur et la biométrie ont révolutionné le domaine de l'application de la loi… La fusion de la biométrie et de l'IA offre à la fois efficacité et précision, permettant d'identifier rapidement et efficacement les criminels tout en protégeant la vie privée des personnes non concernées*[8].

La TRF et les systèmes biométriques peuvent être utilisés à de nombreuses fins et dans de nombreux contextes, notamment :

- pour soutenir les enquêtes criminelles, notamment les menaces terroristes, les enquêtes sur les personnes disparues, dont les enfants, la traite des êtres humains ou l'exploitation sexuelle et les évènements publics ;
- pour parcourir les bases de données de photos signalétiques ;
- pour surveiller les espaces publics, privés ou sécurisés ;
- pour identifier les personnes en temps réel grâce aux caméras corporelles de la police ou aux vidéos prises par des drones ;
- pour analyser les images ou les vidéos recueillies par des tiers[9].

La TRF est largement utilisée par les forces de l'ordre aux États-Unis et dans le monde entier[10]. La TRF la plus connue au Canada est celle de la GRC, qui utilisait Clearview AI, un programme de prélèvement d'images sur Internet, aujourd'hui abandonné[11]. Les services de police de Toronto utilisent également la TRF dans certaines circonstances[12].

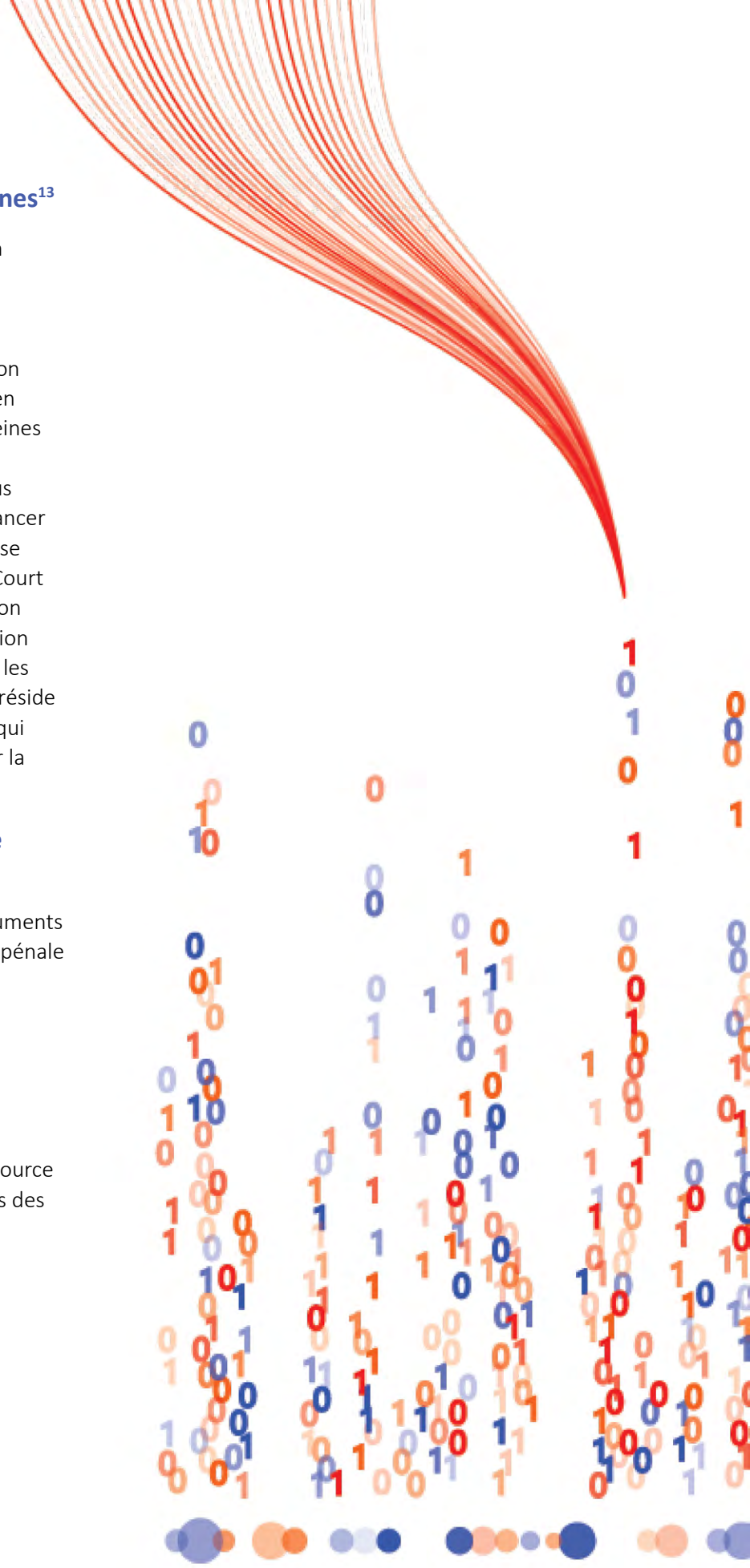
## 4. Algorithmes de mise en liberté sous caution et de détermination des peines[13]

Les algorithmes de mise en liberté sous caution et de détermination des peines sont des outils d'IA ou algorithmiques qui aident les tribunaux pénaux à prendre des décisions en matière de mise en liberté sous caution ou de détermination des peines. L'utilisation d'algorithmes de mise en liberté sous caution et de détermination des peines s'est rapidement répandue aux États-Unis dans les années 2010, où ils sont rapidement apparus comme la « réforme privilégiée » pour faire avancer le mouvement américain de « réforme de la mise en liberté sous caution »[14]. Selon le Center on Court Innovation, un organisme de recherche à but non lucratif basé à New York, « l'intérêt de l'évaluation des risques avant le procès, en particulier dans les systèmes judiciaires importants et surchargés, réside dans la rapidité et l'objectivité de l'évaluation, qui exploite la puissance des données pour faciliter la prise de décision »[15].

## 4. Autres systèmes d'IA utilisés dans le système de justice pénale[16]

Les autres technologies abordées dans les documents thématiques sur l'IA dans le système de justice pénale comprennent :

- les lecteurs automatiques de plaques d'immatriculation ;
- les drones ;
- les systèmes de détection de coup de feu ;
- les systèmes de renseignements d'origine source ouverte (OSINT) et de renseignements issus des réseaux sociaux (SOCINT) ;
- les preuves générées par l'IA.



# 4. L'IA dans le système de justice pénale : risques et problèmes

De nombreux rapports documentent les risques que représentent les systèmes d'IA tels que la surveillance biométrique, le maintien de l'ordre prédictif et les algorithmes de mise en liberté sous caution et de détermination des peines pour les droits de la personne, les libertés civiles, la protection de la vie privée et l'équité procédurale. Ces rapports examinent également comment les risques liés à ces systèmes touchent de manière disproportionnée les communautés et les personnes à faible revenu, autochtones, racisées ou autrement vulnérables. Parmi les risques notables liés à l'IA dans le système de justice pénale, on peut citer les thèmes suivants :

## 1. Préjugés et discrimination

Les problèmes liés au biais de données et à la discrimination dans les systèmes d'IA utilisés dans le système de justice pénale sont bien connus et largement reconnus[17]. Par exemple, des études sur les systèmes de RF « ont clairement démontré les préjugés raciaux et genrés, c'est-à-dire que les femmes et les personnes de couleur sont plus susceptibles d'être mal identifiées par les TRF et, par conséquent, plus susceptibles d'être accusées à tort par les policiers qui les utilisent que les hommes à la peau claire »[18]. De nombreux algorithmes utilisés dans le cadre du maintien de l'ordre prédictif et de la détermination des cautions ou des peines se sont également révélés biaisés et discriminatoires[19].

Les craintes relatives aux préjugés ont donné lieu à de nombreuses propositions visant à règlementer strictement les systèmes d'IA utilisés dans le système de justice pénale[20].

## 2. Vie privée et surveillance

Les risques liés à la vie privée et à la surveillance sont largement reconnus dans les systèmes d'IA criminels, en particulier les systèmes de RF[21]. Les risques liés à la vie privée dans d'autres systèmes d'IA utilisés dans le système de justice pénale peuvent inclure :

- Les systèmes de surveillance des réseaux sociaux qui peuvent réduire la confidentialité des communications en ligne.
- Les lecteurs automatiques de plaques d'immatriculation qui peuvent suivre les déplacements d'une personne.
- Les drones qui surveillent des personnes ou des évènements ou qui sont utilisés pour recueillir des renseignements sur des passants qui ne sont pas liés à une enquête policière[22].

Comme avec les TRF, les risques liés à la vie privée ont également donné lieu à de nombreuses propositions visant à règlementer ou à interdire les applications de l'IA dans le système de justice pénale[23].

## 3. Communication d'informations et transparence

Les systèmes d'IA dans le système de justice pénale sont souvent critiqués pour leur manque de communication et de transparence, notamment[24] :

- Absence de communication sur l'existence d'un système d'IA en général ou à la personne concernée.
- Absence de communication sur les éléments clés d'un système d'IA, tels que ses données d'apprentissage.
- Absence de communication sur la manière dont un système d'IA prend des décisions.

L'utilisation de Clearview AI par la GRC est la controverse la plus connue au Canada en matière de communication d'informations relatives à l'IA[25].

## 4. Opacité/Manque d'explications

Les systèmes d'IA dans le système de justice pénale peuvent intégrer dans leur code un ensemble complexe de décisions juridiques, techniques, statistiques et opérationnelles. La complexité et l'opacité des outils d'IA peuvent rendre les décisions assistées par l'IA « encore plus impénétrables que les jugements humains »[26]. En conséquence, même les systèmes algorithmiques simples peuvent devenir des « boites noires ».

## 5. Exactitude, fiabilité et validité des données

La TRF, le maintien de l'ordre prédictif et d'autres systèmes d'IA utilisés dans le système de justice pénale ont fait l'objet de vives critiques quant à l'exactitude, à la fiabilité et à la validité des données utilisées pour leur apprentissage[27].

## 6. Surveillance efficace

Les systèmes d'IA dans le système de justice pénale soulèvent plusieurs risques en matière de surveillance, notamment :

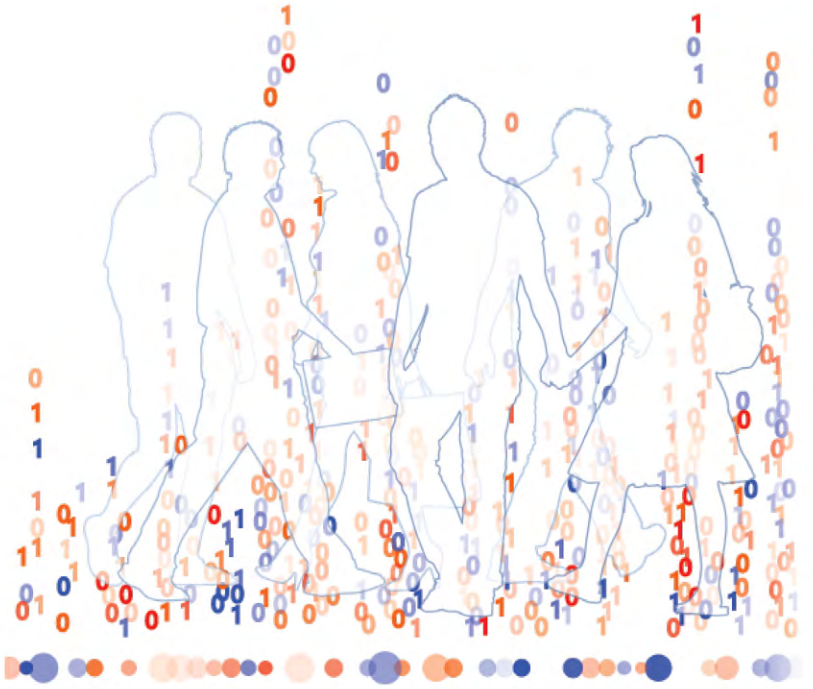
- **Lacunes en matière de gouvernance.** Sans politiques juridiques claires et cohérentes et sans barrière de protection, il pourrait y avoir des lacunes dans la responsabilité juridique de l'IA. Par exemple, tous les services de police ne disposeraient pas nécessairement de politiques en matière d'IA.
- **Contrôle judiciaire incohérent ou incomplet.** Faute de règles cohérentes, les tribunaux pourraient être amenés à trancher au cas par cas des questions complexes liées à l'IA, ce qui risquerait d'entrainer une surveillance incohérente ou incomplète, des retards et une augmentation des couts liés aux litiges.
- **Perte de l'indépendance judiciaire/réduction du pouvoir discrétionnaire.** Une dépendance excessive à l'égard des prédictions de l'IA peut compromettre l'apparence ou la réalité de l'indépendance judiciaire. Le biais d'automatisation peut conduire les décideurs à limiter leur pouvoir discrétionnaire, même lorsqu'il y a une « intervention humaine ».
- **Manque d'engagement du public.** De nombreux systèmes d'IA dans le système de justice pénale ont été critiqués par des communautés qui estiment ne pas avoir été consultées ni informées au sujet de systèmes qui les concernent.

Ces risques pourraient porter atteinte aux droits garantis par la *Charte*, à l'équité procédurale, à la fiabilité de la preuve et à la jurisprudence.

## 7. Erreurs judiciaires/Accès à la justice

Tous les risques susmentionnés pourraient entrainer des erreurs judiciaires à l'égard des personnes accusées, notamment des risques d'arrestation arbitraire, de détention illégale et de violation des droits garantis par la *Charte*, du droit à la vie privée et du droit à une procédure équitable.

Les systèmes d'IA dans le système de justice pénale soulèvent également des préoccupations systémiques en matière d'accès à la justice, notamment la manière dont les personnes accusées (en particulier celles qui sont représentées par un avocat de l'aide juridique ou qui se représentent elles-mêmes) pourront contester efficacement les systèmes d'IA.



# 5. Les avantages et les risques de l'IA en contexte

Lorsqu'on évalue les avantages et les risques de l'IA dans le système de justice pénale, il est important de tenir compte des variations au sein de ces systèmes et entre eux. Ces variations peuvent avoir des implications très diverses pour la sécurité publique, les enquêtes policières et les droits individuels. Par exemple, tous les systèmes de reconnaissance faciale comportent des risques en matière de surveillance, mais l'ampleur de ces risques dépend en grande partie de la manière dont les images sont recueillies, du lieu où elles le sont et de la base de données à laquelle elles sont comparées. Il existe également de nombreuses variations au sein des systèmes de maintien de l'ordre prédictif et entre eux[28].

Il est également important de noter que les technologies d'IA dans le système de justice pénale ne sont pas statiques. Par exemple, un rapport récent de l'Académie nationale des sciences des États-Unis souligne que le maintien de l'ordre prédictif évolue et que bon nombre des premiers systèmes de maintien de l'ordre prédictif « ont fait leur temps » face à de vives critiques[29].

# 6. Aperçu des documents thématiques du projet sur l'IA dans le système de justice pénale

Le projet de la CDO sur l'IA dans le système de justice pénale comprend une introduction et quatre documents thématiques. Chaque document thématique examine l'utilisation de l'IA dans une phase distincte du processus pénal.

Tous les documents thématiques sont disponibles sur le site Web du projet de la CDO.

## Rapport 1 : Introduction au projet de la CDO sur l'IA dans le système de justice pénale

Le premier document est une introduction et un résumé du projet de la CDO sur l'IA dans le système de justice pénale. Ce rapport a été rédigé par le directeur général de la CDO, Nye Thomas.

Ce rapport cerne les systèmes d'IA actuellement utilisés dans le secteur de la justice pénale et résume leurs avantages et leurs risques respectifs. Il résume également les initiatives internationales et canadiennes en matière de gouvernance de l'IA dans le secteur pénal. Il se termine par une évaluation de la « fiabilité de l'IA dans le système de justice pénale » au Canada et en Ontario.

## Rapport 2 : L'utilisation de l'IA par les forces de l'ordre

Le deuxième document du projet examine l'utilisation de l'IA par les forces de l'ordre. Ce document a été rédigé par Ryan Fritsch, avocat à la CDO.

Ce rapport traite du large éventail de technologies basées sur l'IA utilisées par les forces de l'ordre à l'échelle internationale et au Canada, notamment la reconnaissance faciale, le maintien de l'ordre prédictif, la reconnaissance d'objets, les preuves générées par l'IA et autres. Il examine les avantages et les risques de ces systèmes et la manière dont ils soulèvent de nouvelles questions juridiques, sociétales et constitutionnelles.

Le rapport examine également comment l'IA pourrait influencer l'évaluation des accusations par le ministère public et la fonction consultative entre le ministère public et les forces de l'ordre, y compris les questions relatives à la recevabilité de l'IA, aux exigences en matière de divulgation et aux questions de confidentialité.

## Rapport 3 : L'IA et l'évaluation du risque associé à la mise en liberté sous caution, à la détermination des peines et à la récidive

Le troisième document du projet traite de l'IA, des algorithmes et de la mise en liberté sous caution. Les auteurs de ce document sont Armando D'Andrea, responsable du comité pénal et ancien avocat de service en matière criminelle, Aide juridique Ontario et Gideon Christian, faculté de droit, Université de Calgary.

Les décisions relatives à la mise en liberté sous caution, à la détermination des peines et aux mesures postérieures au prononcé d'une sentence s'appuient depuis longtemps sur des évaluations professionnelles des risques afin de prédire le danger potentiel qu'un accusé ou un délinquant représente pour le public. Cependant, les évaluations des risques basées sur l'IA apportent de nouvelles complications, telles que l'impossibilité de contrinterroger les algorithmes en boite noire ; la déférence à la technologie lorsque les humains s'en remettent excessivement aux recommandations générées par l'IA ; la nécessité d'équilibrer la protection des secrets commerciaux, les droits garantis par la *Charte* et le droit à l'application régulière de la loi ; et le risque que les systèmes d'IA perpétuent les préjugés systémiques racistes et colonialistes.

Le rapport examine également la nature particulière des audiences de mise en liberté sous caution, qui ont tendance à être plus rapides et informelles, ainsi que des audiences de détermination des peines et des audiences postérieures au prononcé d'une sentence, dans lesquelles la présomption d'innocence ne s'applique plus.

## Rapport 4 : L'IA durant le procès et en appel

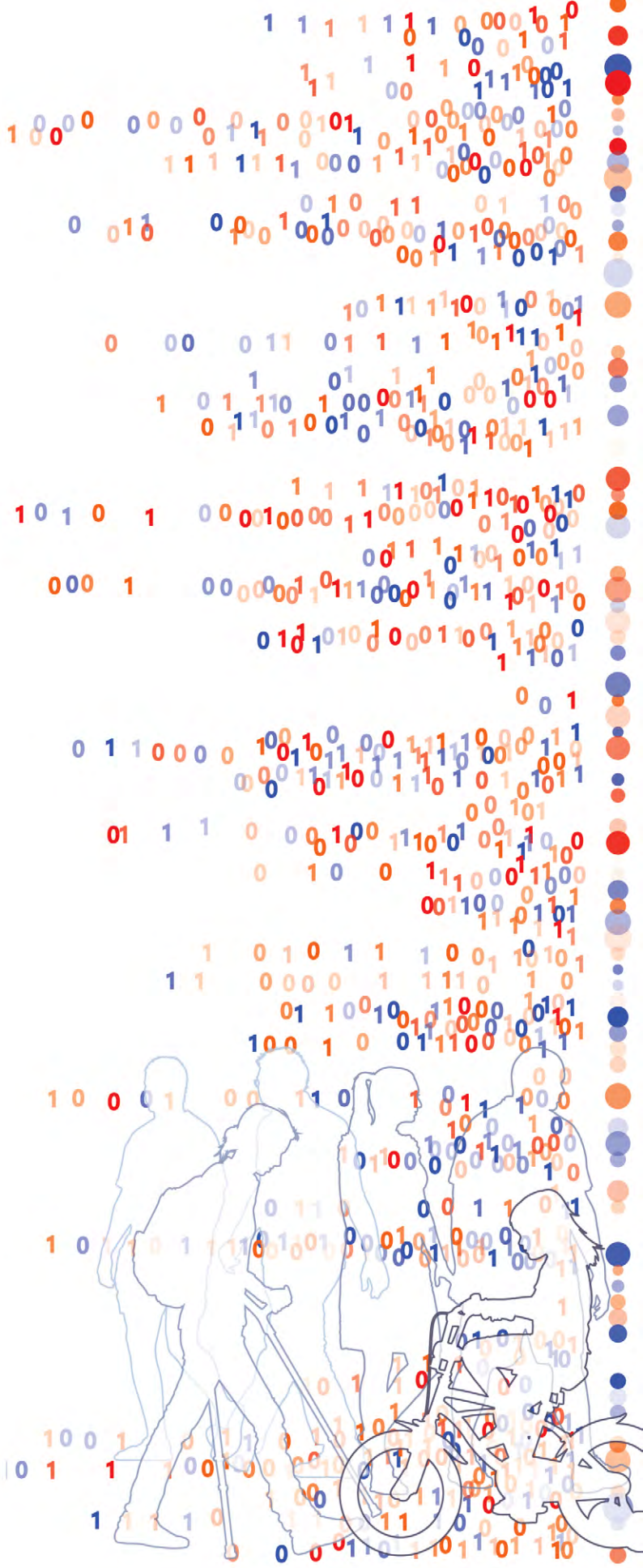
Le quatrième document du projet traite de l'IA dans les procès pénaux et les procédures d'appel. Ce document a été rédigé par Paula Thompson, Initiatives stratégiques, ministère du Procureur général, et par Eric Neubauer, avocat de la défense, Neubauer Law, et coprésident, Criminal Lawyers Association Technology Committee.

L'IA soulève de nouvelles questions fondamentales pour garantir l'équité des procès et la protection de la liberté et des droits constitutionnels. Les procès et les appels garantissent une procédure équitable et transparente en s'appuyant sur la *Charte des droits et libertés*, les principes de common law qui régissent l'interprétation des cas et l'équité procédurale, ainsi que le droit de la preuve. L'introduction de l'IA, tant comme preuve que comme outil d'analyse utilisé par les parties au litige et les fonctionnaires judiciaires, soulève de nouvelles préoccupations en matière de divulgation, de recevabilité, de partialité et d'accès à la justice, qui ne sont pas directement abordées par la législation et la jurisprudence existantes.

## Rapport 5 : L'IA et les mécanismes de surveillance systémique

Le dernier document du projet traite de la surveillance systémique. Les auteurs de ce document sont Brenda McPhail, conseillère principale en technologie et en politiques, bureau de la Commissaire à l'information et à la protection de la vie privée de l'Ontario; Marcus Pratt, conseiller principal, Service des politiques, Aide juridique Ontario et Jagtaran Singh, conseiller juridique, Commission ontarienne des droits de la personne.

Sans cadres juridiques, règlementaires et politiques solides, le droit pénal est limité dans sa capacité à superviser l'utilisation de l'IA par les acteurs étatiques et à atténuer les abus potentiels. Bien que le projet de loi fédéral C-27 et la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique* (*LRSCN*) de l'Ontario contiennent certaines mesures règlementaires importantes, leur application au droit pénal est limitée. Parmi les principaux problèmes, citons l'absence de recours en cas de violation des droits, l'absence d'organismes de contrôle indépendants et la conception relativement restrictive des droits à la vie privée qui ressort de la législation et de la jurisprudence actuelles. Les nouvelles lois et les projets de loi de certaines juridictions, comme l'Union européenne et les États-Unis, peuvent offrir des pistes, mais ces approches présentent également des lacunes. De plus, le document examine comment l'IA mettra à l'épreuve le droit à une défense complète et à l'accès à la justice, notamment le temps et les ressources financières nécessaires aux avocats de la défense pour contester l'utilisation de l'IA dans le cadre de la mise en liberté sous caution ou de la détermination des peines, ou l'admission de preuves issues de l'IA lors d'un procès.



# 7. Une IA fiable dans le système de justice pénale

Les avantages, les risques et les préjudices potentiels de l'IA dans le système de justice pénale sont largement reconnus par les gouvernements, les services de police, les procureurs, les avocats de la défense, les universitaires et les ONG du monde entier[30]. Cette reconnaissance a donné lieu à un large éventail de lois, de politiques et de cadres fondés sur le principe selon lequel les avantages de l'IA dépendent de règles spécifiques et complexes qui atténuent les risques et les préjudices.

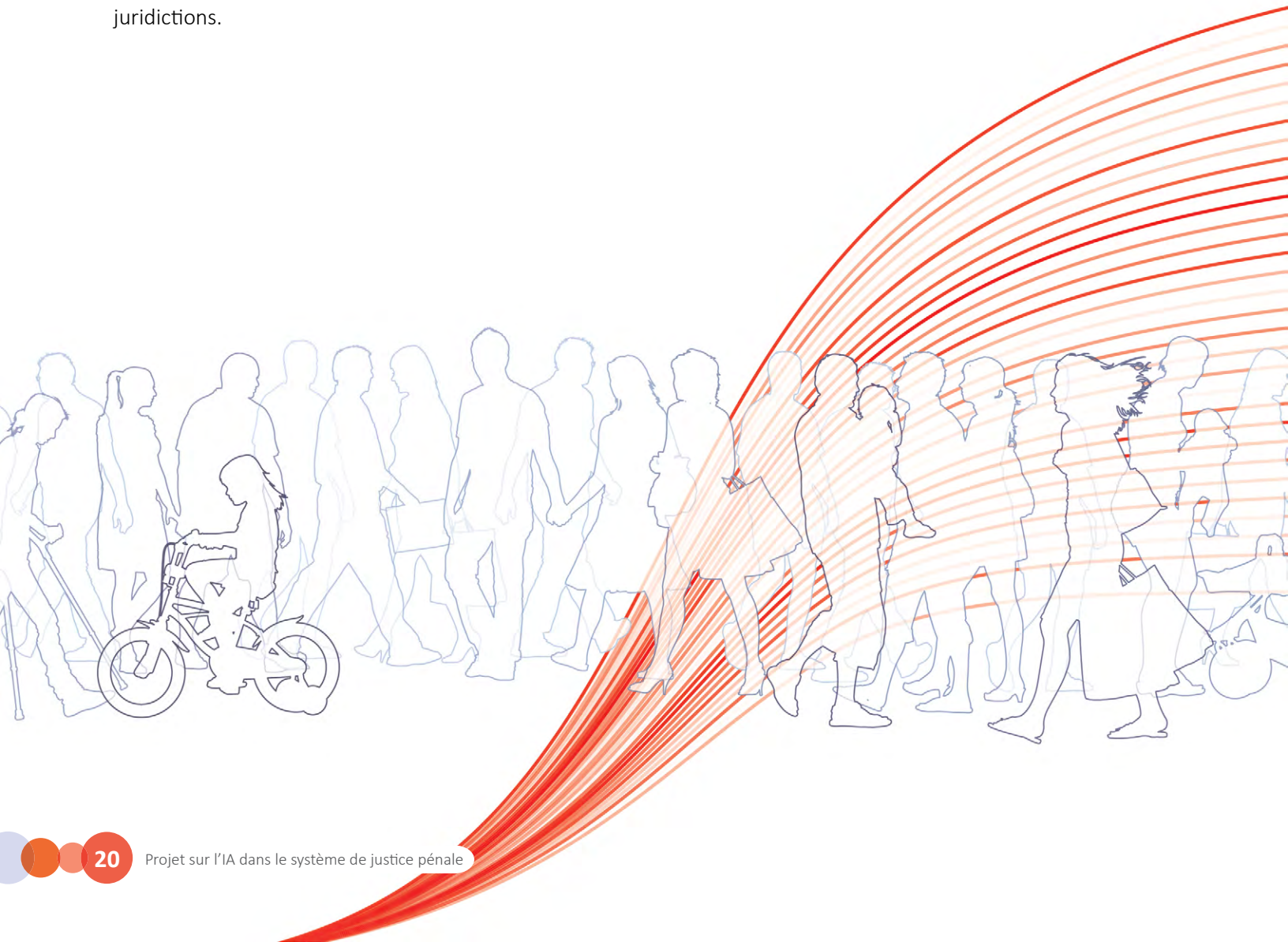
Il existe un large éventail d'initiatives en matière d'IA fiable dans le système de justice pénale en Europe et aux États-Unis. Par exemple, le règlement sur l'intelligence artificielle de l'Union européenne (règlement de l'UE sur l'IA) contient des interdictions relatives à plusieurs systèmes d'IA dans le secteur pénal, notamment la surveillance biométrique en temps réel et certains systèmes de maintien de l'ordre prédictif[31]. Le règlement de l'UE sur l'IA identifie également plusieurs outils d'IA utilisés dans le domaine de « l'application de la loi » et de « l'administration de la justice » comme présentant un risque élevé et donc soumis à des exigences règlementaires plus détaillées[32]. Aux États-Unis, une législation détaillée sur l'IA dans le système de justice pénale, des décrets, des politiques et des règles ont été adoptés ou proposés par le gouvernement fédéral, les États, les municipalités, les services de police et des ONG[33].

Le thème général de ces initiatives est qu'il est nécessaire de disposer de règles cohérentes et complètes pour garantir que les systèmes d'IA dans le secteur pénal soient bénéfiques, légaux et responsables. Cela dit, le contenu et la forme de ces initiatives varient considérablement et peuvent inclure ce qui suit :

- Communication obligatoire des systèmes d'IA dans le secteur pénal, y compris des « registres publics d'IA ».
- Interdiction des systèmes d'IA présentant le plus haut risque dans le secteur pénal.
- Critères permettant d'identifier les systèmes interdits ou à haut risque.
- Limitations de la finalité et de l'utilisation.
- Évaluations obligatoires et transparentes de l'incidence de l'IA.
- Exigences en matière d'atténuation.
- Obligations obligatoires de mesurer, de corriger et de contrôler les biais dans les systèmes d'IA.

- Garanties procédurales, telles que l'obligation d'obtenir un mandat pour les systèmes à haut risque.
- Exigences obligatoires en matière d'intervention humaine et d'apprentissage.
- Exigences obligatoires en matière d'audit et d'évaluation.
- Surveillance indépendante des systèmes individuels et gouvernementaux en matière d'IA en général.

Pour la CDO, ni le Canada ni l'Ontario ne devrait adopter de jurisprudence ou de cadre unique. Les lois et les politiques en matière d'IA fiable dans le système de justice pénale doivent être adaptées à nos lois, à notre système de justice pénale et à nos institutions. La CDO estime que les décideurs politiques et les parties prenantes du Canada peuvent tirer d'importantes leçons de l'expérience d'autres juridictions.



# 8. Une IA fiable dans le système de justice pénale canadien

## Lois et politiques existantes

Les documents thématiques du projet de la CDO analysent comment les protections existantes prévues par la *Charte*, le *Code criminel*, les lois sur les droits de la personne, les règles de common law, la procédure pénale et les règles de preuve peuvent être ou seront utilisées pour répondre aux défis posés par l'IA à chaque étape du processus de justice pénale. Les documents thématiques présentent une analyse complète des forces et des lacunes de ce cadre juridique complexe.

La CDO et nos auteurs ont conclu que, bien que les règles et procédures juridiques existantes présentent de nombreux avantages, elles ne permettent pas d'établir une IA fiable dans le système de justice pénale au Canada. En effet :

- L'IA soulève des questions nouvelles, complexes et lourdes de conséquences à chaque étape d'une procédure pénale.
- Des systèmes d'IA mal conçus ou mal utilisés pourraient avoir des répercussions profondes sur les libertés individuelles, les droits constitutionnels, la vie privée, la procédure pénale, l'efficacité des tribunaux, l'accès à la justice et la confiance du public dans le système de justice pénale canadien.
- Il est nécessaire de garantir la responsabilité de l'IA à chaque étape du système de justice pénale.
- La « judiciarisation des conflits » n'est guère susceptible de relever efficacement les défis systémiques et complexes que posent les systèmes d'IA utilisés dans le secteur pénal.
- Il n'est pas certain que les organismes et les tribunaux seront en mesure de déterminer ou d'appliquer de manière cohérente les obligations en matière de divulgation de l'IA, les tests de partialité et de confidentialité, les critères de fiabilité, etc.
- La CDO et nos auteurs craignent que ces problèmes ne se propagent et ne s'aggravent à travers le réseau vaste, diversifié et décentralisé des institutions et des acteurs impliqués dans le développement, l'exploitation, les litiges ou la supervision de l'IA dans le système de justice pénale du Canada et de l'Ontario.

## Législation fédérale sur l'IA, directives et politiques gouvernementales

Il existe trois initiatives au niveau fédéral qui concernent les systèmes d'IA dans le système de justice pénale.

### 1. La Loi sur l'intelligence artificielle et les données *(LIAD)*

En juin 2022, le ministre fédéral de l'Industrie, des Sciences et du Développement économique (ISDE) a présenté le projet de loi C-27, intitulé *Loi sur l'intelligence artificielle et les données* (*LIAD*)[34].

À l'instar du règlement de l'UE sur l'IA, la *LIAD* proposait une approche fondée sur les risques pour la gouvernance de l'IA. Cependant, contrairement au règlement de l'UE sur l'IA, la *LIAD* ne règlementait pas directement l'utilisation de l'IA dans le secteur public ou le système de justice pénale. Elle se serait plutôt appliquée aux organisations du secteur privé responsables de « concevoir, de développer, d'utiliser ou de rendre disponible un système d'IA »[35]. À l'origine, la *LIAD* ne comprenait pas non plus d'interdictions ou de restrictions explicites concernant les systèmes d'IA présentant des risques inacceptables.

Lors de son introduction, la *LIAD* a été vivement critiquée pour son manque de détails, de consultations et de protections importantes en matière d'IA fiable[36]. Le gouvernement fédéral a répondu, en partie, en proposant plusieurs modifications, notamment une liste de « classes de systèmes qui seraient considérés comme ayant une incidence élevée », dont trois pertinentes pour la justice pénale (certains systèmes biométriques, les systèmes d'IA utilisés par les tribunaux et les systèmes d'IA « destinés à assister un agent de la paix… »)[37]. Les modifications proposées par le gouvernement fédéral n'ont pas apaisé les détracteurs de la *LIAD*, qui ont continué à décrier la législation[38].

La *LIAD* n'a pas été adoptée par le gouvernement fédéral avant la prorogation du Parlement en janvier 2025.

### 2. La directive fédérale sur la prise de décisions automatisée

En 2021, le gouvernement fédéral a promulgué la directive sur la prise de décisions automatisée (directive fédérale sur la PDA) et son complément, l'évaluation de l'incidence algorithmique (EIA). La directive fédérale sur la PDA et l'EIA s'appliquent à un large éventail de systèmes technologiques fédéraux, et pas seulement aux systèmes d'IA[39].

La CDO a beaucoup écrit à propos de la directive fédérale sur la PDA et l'EIA[40]. Nous avons salué ces deux documents comme des exemples phares d'outils et de stratégies qui intègrent des garanties d'équité procédurale dans la conception et le fonctionnement des processus décisionnels automatisés du gouvernement[41]. La directive fédérale sur la PDA et l'EIA ne s'appliquent pas aux organismes fédéraux chargés de l'application de la loi[42].

Le gouvernement fédéral procède actuellement à son quatrième examen de la directive fédérale sur la PDA et de l'EIA[43]. Cet examen pourrait inclure des propositions visant à renforcer les dispositions relatives aux droits de la personne de la directive fédérale sur la PDA et à établir des critères plus explicites concernant les systèmes d'IA prohibés au niveau fédéral. Cette révision n'appliquera pas la directive fédérale sur la PDA et l'EIA aux organismes fédéraux chargés de l'application de la loi.

### 3. GRC

En réponse au rapport spécial du Commissariat à la protection de la vie privée sur l'utilisation de Clearview AI par la GRC, cette dernière a créé le Programme national d'intégration des technologies (PNIT)[44]. Le PNIT est un programme interne visant à évaluer les systèmes technologiques de la GRC. La GRC affirme que l'IA et les technologies intrusives pour la vie privée sont les priorités absolues du PNIT[45].

Le premier rapport sur la transparence du PNIT, intitulé *Plan de transparence : Aperçu des technologies opérationnelles*, a été publié en septembre 2024[46]. Le *Plan de transparence* décrit comment la GRC met en œuvre une approche plus proactive en matière d'évaluation des technologies et de transparence, y compris les systèmes d'IA. La GRC indique que le PNIT avait évalué 28 technologies en septembre 2024[47].

### 4. Évaluation des initiatives fédérales visant à promouvoir une IA fiable dans le secteur de la justice pénale

Si elle avait été adoptée, une version révisée de la *LIAD* aurait inclus des dispositions limitées visant à promouvoir une IA fiable dans le secteur de la justice pénale au Canada. L'ajout de systèmes d'IA « à incidence élevée » dans les domaines de la biométrie, des tribunaux et des services de police aurait constitué un complément utile à la législation. Parmi les autres aspects positifs de la *LIAD* figuraient l'obligation de publication et de notification en langage clair, l'obligation de prendre des mesures pour prévenir et atténuer les préjugés, et des sanctions importantes en cas de non-respect. Néanmoins, une version modifiée de la *LIAD* n'aurait toujours pas établi une IA fiable dans le domaine de l'application de la loi fédérale ou du système de justice pénale.

La directive fédérale sur la PDA et l'EIA restent des exemples phares de la manière de garantir l'équité des procédures dans les systèmes d'IA du secteur public. La révision actuelle de la directive fédérale sur la PDA et de l'EIA pourrait renforcer encore ces instruments. Ces propositions, bien que bienvenues, ne permettraient toujours pas d'appliquer la directive fédérale sur la PDA et l'EIA aux organismes fédéraux chargés de l'application de la loi.

L'inaction du gouvernement fédéral dans ce domaine est décevante. Cela fait environ cinq ans que la première directive fédérale sur la PDA a été promulguée, mais il n'existe toujours pas de législation, de directive ou de politique fédérale spécifique établissant une IA fiable pour les institutions ou les acteurs de la justice pénale fédérale, y compris les services fédéraux chargés de l'application de la loi. L'absence d'action au niveau fédéral contraste défavorablement avec l'UE et les États-Unis, qui ont tous deux pris des mesures importantes pour faire face aux risques uniques et graves liés à l'IA dans le secteur pénal.

Le PNIT de la GRC et son récent *Plan de transparence* sont des initiatives complexes qui intègrent bon nombre des principes relatifs à la fiabilité de l'IA dans le secteur de la justice pénale. Cependant, ni le PNIT ni le *Plan de transparence* ne semblent inclure d'informations détaillées sur les utilisations interdites, les catégories de risques ou les exigences en matière d'atténuation. La CDO espère que ces questions seront abordées dans les futures politiques de la GRC.

## Législation, directives gouvernementales et politiques en matière d'IA en Ontario

Il existe trois initiatives en Ontario qui concernent les systèmes d'IA utilisés dans le secteur pénal.

### 1. *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique*

Le gouvernement de l'Ontario a adopté la *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique (LRSCN)* en novembre 2024[48]. L'objectif de la *LRSCN* est « … [d'é]tablir une définition de l'intelligence artificielle (IA) pour favoriser la cohérence au sein du secteur public et d'établir des mesures de protection en vue d'une utilisation responsable des systèmes d'IA »[49].

La CDO a beaucoup écrit sur la *LRSCN* et le projet de loi 194, qui a introduit la législation[50]. Nous avons conclu que la législation ne parvient pas à établir une IA fiable et détaillée pour les systèmes d'IA du secteur public en Ontario en raison de l'absence de protections des droits de la personne, d'exigences en matière de divulgation, de catégories de risques et d'autres dispositions. La *LRSCN* ne s'applique pas à l'IA utilisée dans le système de justice pénale de l'Ontario[51].

## 2. Directive sur l'utilisation responsable de l'IA

Après la *LRSCN,* le gouvernement provincial a publié, en décembre 2024, sa « directive sur l'utilisation responsable de l'intelligence artificielle » (directive de l'Ontario sur l'IA)[52]. La directive de l'Ontario sur l'IA est plus exhaustive que la *LRSCN* et répond à plusieurs préoccupations actuelles de la CDO concernant la politique provinciale en matière d'IA.

Malgré les points forts de la directive de l'Ontario sur l'IA, l'analyse préliminaire de la CDO révèle qu'elle comporte plusieurs lacunes ou ambigüités importantes[53]. Par exemple, la directive :

- ne s'applique explicitement à aucun organisme d'application de la loi ni service de police en Ontario;
- n'établit pas de critères ou d'interdictions cohérents ou transparents en matière de risques liés à l'IA;
- n'établit pas d'obligations de divulgation cohérentes ou exhaustives;
- n'établit pas de régime de recours et ne prévoit pas de dispositions relatives à l'accès à la justice.

## 3. Politique relative à l'utilisation des technologies d'IA de la Commission de services policiers de Toronto

La politique la plus importante en matière d'IA dans le système de justice pénale au Canada est la politique relative à l'utilisation des technologies d'IA (la « Politique sur l'IA de la CSPT ») de la Commission de services policiers de Toronto (CSPT)[54].

La Politique sur l'IA de la CSPT intègre de nombreux principes en matière d'IA fiable dans le secteur de la justice pénale. Par exemple, la Politique sur l'IA de la CSPT :

- Reconnait que la technologie peut soulever de nouvelles préoccupations en matière de « vie privée et de droits (y compris les droits à la liberté d'expression, à la liberté d'association et à la liberté de réunion, à la dignité et à l'égalité des personnes concernées par [les applications de l'IA] »[55].
- Nécessite une technologie conforme à des principes directeurs détaillés, notamment la légalité, l'équité, la fiabilité, la justifiabilité, la responsabilité personnelle et organisationnelle, la transparence, la confidentialité et l'engagement significatif[56].
- Comprend des critères de risque explicites, notamment les « technologies à risque extrêmement élevé » qui ne peuvent être envisagées pour adoption, y compris les systèmes d'IA qui entrainent une « surveillance de masse définie comme le contrôle d'une population ou d'une partie importante d'une population… » et « toute application connue ou susceptible de causer un préjudice ou d'avoir une incidence sur les droits individuels, malgré l'utilisation de techniques d'atténuation, en raison de biais ou d'autres défauts »[57].
- Comprend les obligations relatives aux limitations des finalités, aux exigences en matière de données, aux exigences de divulgation, aux procédures d'approbation et de notification, aux analyses d'incidence et aux stratégies d'engagement du public.

La CSPT a publié son premier rapport d'information publique en janvier 2024. Ce rapport a révélé que la CSPT utilise cinq systèmes basés sur l'IA. La CSPT a également évalué elle-même le niveau de risque de chaque système. Un système de RF qui automatise l'identification des photos signalétiques était le seul système classé comme « à haut risque »[58].

Au moins un autre service de police de l'Ontario a adopté une politique en matière d'IA. En octobre 2024, le Conseil des services de la police régionale de Durham a adopté une politique sur l'utilisation de l'intelligence artificielle[59]. Cette politique comprend plusieurs principes en matière d'IA fiable dans le secteur de la justice pénale, mais elle est moins détaillée et moins prescriptive que la politique de la CSPT en matière d'IA. Par exemple, la politique de Durham ne comprend pas de catégories de risques ni d'interdictions de « technologies à risque extrêmement élevé ».

## 4. Évaluation des initiatives provinciales visant à promouvoir la fiabilité de l'IA dans le secteur de la justice pénale

Le gouvernement provincial a pris des premières mesures importantes pour promouvoir la fiabilité de l'IA dans l'ensemble du secteur public de l'Ontario. À ce jour, cet engagement ne s'étend pas aux systèmes d'IA utilisés dans les services provinciaux chargés de l'application de la loi ou dans le système provincial de justice pénale. Par conséquent, il n'existe aucune loi, directive ou politique spécifique établissant la fiabilité de l'IA dans le système de justice pénale de l'Ontario.

La *LRSCN* n'établit pas de cadre complet pour la fiabilité de l'IA dans les systèmes d'IA du secteur public provincial en général ni dans le système de justice pénale en particulier.

La directive de l'Ontario sur l'IA est plus détaillée que la *LRSCN*, mais de nombreuses questions restent en suspens. Il est important de noter que la directive de l'Ontario sur l'IA ne s'applique à aucun service de police de l'Ontario.

La politique en matière de fiabilité de l'IA dans le système de justice pénale la plus substantielle en Ontario est la politique de la CSPT sur l'IA. Il s'agit d'un document complexe qui intègre de nombreux principes relatifs à la fiabilité de l'IA dans le secteur de la justice pénale identifiés par la CDO et d'autres juridictions. Toutefois, la politique de la CSPT sur l'IA présente certaines limites structurelles qui font obstacle à son utilisation comme outil de gouvernance d'une IA fiable dans le secteur de la justice pénale.

D'abord, la politique de la CSPT en matière d'IA n'est pas juridiquement contraignante. Elle ne crée pas de régime de responsabilité juridique, ni de dispositions correctives ou de sanctions en cas de non-respect.

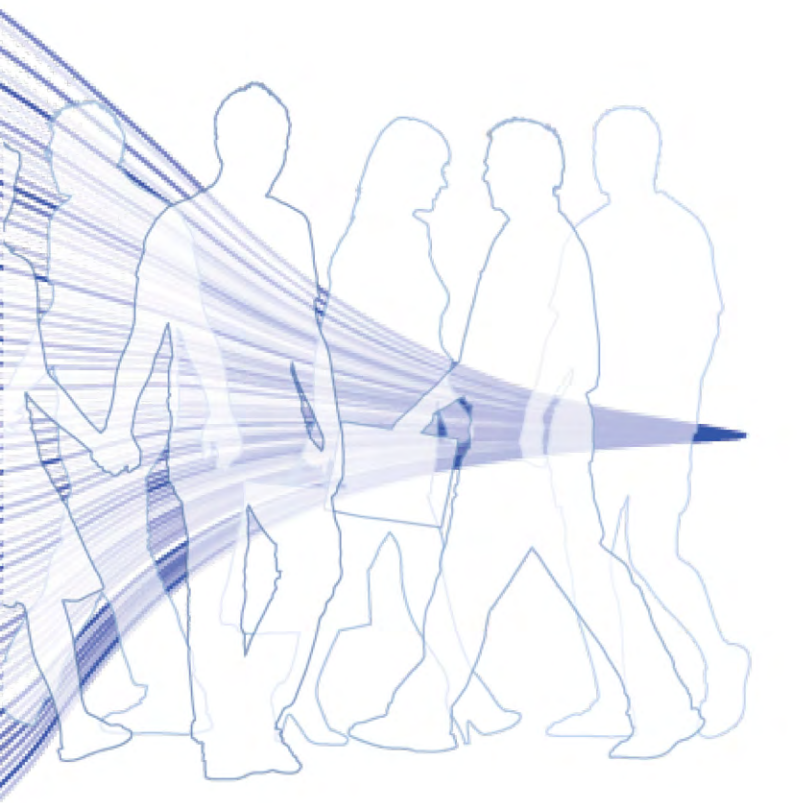
Ensuite, la politique de la CSPT en matière d'IA est autorégulée. Elle ne crée pas d'organisme de surveillance indépendant ni de mécanisme d'examen externe. En conséquence, la CSPT a été critiquée pour son interprétation laxiste de sa politique en matière d'IA[60].

Enfin, et surtout, la politique de la CSPT en matière d'IA est une politique administrative qui régit un seul service de police en Ontario. Elle n'établit pas de norme provinciale en matière d'IA pour les services de police en général ni pour aucun autre élément du système de justice pénale de l'Ontario.

Du point de vue provincial, la politique de la CSPT en matière d'IA souligne les défis et les dangers de déléguer la règlementation des systèmes d'IA utilisés dans le domaine policier aux services de police et aux commissions individuelles : l'Ontario compte 53 services de police. À ce jour, seuls deux services semblent avoir adopté des politiques spécifiques en matière d'IA. Cela signifie que 51 services de police en Ontario ne sont soumis à aucune interdiction, à aucun critère de risque ni à aucune exigence de divulgation et de consultation en matière d'IA. Par conséquent, l'un ou plusieurs des 51 services de police pourraient adopter des systèmes d'IA à « risque extrême » (tels que la reconnaissance faciale en temps réel ou le maintien de l'ordre prédictif) sans barrières de protection efficaces, sans obligation de rendre des comptes et sans divulgation publique. Il s'agit là du pire scénario, mais il n'est pas impossible.

De plus, les services de police ne sont pas les seules institutions ou acteurs provinciaux de la justice pénale susceptibles d'être touchés par les systèmes d'IA. Il y a aussi les ministères du Solliciteur général et du Procureur général, les tribunaux, les procureurs de la Couronne, les avocats de la défense, Aide juridique Ontario et d'autres. En avril 2025, il n'y avait pas de lois ou de règles spécifiques régissant l'utilisation ou l'interprétation des systèmes d'IA dans le secteur pénal par ces organisations.

Sans intervention provinciale, toutes ces institutions devront élaborer leurs propres politiques en matière d'IA. Ces politiques peuvent être cohérentes ou non, respecter ou non les règles juridiques existantes, protéger ou non les droits et intégrer ou non des principes de fiabilité en matière d'IA dans le secteur pénal. Malheureusement, l'expérience montre que des règles fragmentées ou variables en matière d'IA dans le secteur pénal peuvent exposer les habitants de certaines régions de la province à un risque accru de discrimination fondée sur l'IA, d'arrestations arbitraires, de violations de la vie privée, etc.



## Directives des commissaires à la protection de la vie privée et des tribunaux canadiens

Les commissaires à la protection de la vie privée et les tribunaux canadiens constituent une dernière source de politiques en matière de fiabilité de l'IA dans le secteur de la justice pénale.

Les commissaires à la protection de la vie privée du Canada ont joué un rôle de premier plan dans la promotion de la fiabilité de l'IA dans le secteur de la justice pénale au Canada. À ce jour, les commissaires à la protection de la vie privée du Canada ont réalisé au moins cinq études ou rapports sur les technologies de reconnaissance faciale dans les services de police canadiens[61]. Ces rapports fournissent des directives détaillées sur la manière dont les services de police peuvent utiliser les systèmes d'IA tout en respectant le droit à la vie privée. La CDO espère que les commissaires à la protection de la vie privée du Canada continueront à se pencher sur les questions liées à l'IA dans le système de justice pénale.

Outre les commissaires à la protection de la vie privée, plusieurs tribunaux canadiens ont adopté des politiques en matière d'IA. Par exemple, la Cour fédérale a adopté des politiques visant à encadrer l'utilisation de l'IA par la Cour et à orienter l'utilisation de l'IA par les parties et les professionnels qui comparaissent devant elle[62]. Les tribunaux de l'Alberta, du Manitoba et du Québec ont adopté des politiques similaires[63]. Enfin, le Conseil canadien de la magistrature a produit un ensemble de lignes directrices bien pensées intitulées *Lignes directrices sur l'utilisation de l'intelligence artificielle dans les tribunaux canadiens*[64]. Ces lignes directrices soulignent la nécessité de maintenir et de respecter l'indépendance judiciaire lorsque les tribunaux mettent en œuvre des systèmes d'IA.

Les directives des commissaires à la protection de la vie privée et des tribunaux constituent des efforts importants pour établir des principes en matière de fiabilité de l'IA dans leurs domaines respectifs. Elles n'établissent toutefois pas de responsabilité globale pour les systèmes d'IA dans le secteur pénal, que ce soit à l'échelle nationale ou provinciale.

# 9. Conclusion

De nombreux progrès ont été réalisés en matière de gouvernance de l'IA à l'échelle fédérale et provinciale au Canada. Il faut saluer les efforts déployés par plusieurs services de police, commissaires à la protection de la vie privée et autres intervenants canadiens, qui ont pris d'importantes initiatives pour lutter contre les risques liés à l'IA dans le système de justice pénale. Malheureusement, il existe encore des lacunes importantes et lourdes de conséquences dans le cadre législatif ou juridique régissant les systèmes d'IA dans le secteur pénal, notamment :

- **Absence d'exigences obligatoires et cohérentes en matière de divulgation.** À l'heure actuelle, la grande majorité des services de police de l'Ontario pourraient mettre en œuvre le maintien de l'ordre prédictif, la technologie de reconnaissance faciale ou d'autres formes d'IA sans avoir à en informer le public.
- **Absence d'interdictions relatives à l'IA en matière pénale, de « barrière de protection » ou de critères de risque cohérents.** En Ontario, il n'existe aucune « barrière de protection » légale interdisant ou règlementant les systèmes d'IA dans le secteur pénal les plus risqués, tels que la surveillance de masse en temps réel et le maintien de l'ordre prédictif. Il n'existe pas non plus de catégories de risques transparentes et cohérentes permettant d'identifier de manière systématique les risques liés à l'IA dans le secteur pénal et les stratégies d'atténuation de ces risques.
- **Absence d'évaluations d'incidence obligatoires.** Il n'existe aucune obligation provinciale pour les acteurs du système de justice pénale d'évaluer l'incidence d'un système d'IA sur les droits garantis par la *Charte*, les droits de la personne, la vie privée ou la justice procédurale.
- **Absence de garanties procédurales pénales.** Au Canada (et par extension, en Ontario), il n'existe aucune protection procédurale explicite régissant l'utilisation par la police ou les tribunaux de systèmes d'IA dans le secteur pénal à haut risque, telle que l'obligation d'obtenir un mandat pour utiliser ces systèmes. Il n'existe pas non plus de politiques ou de programmes visant à garantir le droit à une défense complète, à une représentation juridique efficace ou à l'accès à la justice.
- **Absence d'obligation obligatoire de tester, d'auditer ou d'évaluer les systèmes d'IA dans le secteur pénal.** Un système d'IA pourrait être mis en œuvre dans le système de justice pénale de l'Ontario sans obligation de vérifier ou d'évaluer son exactitude, son impartialité, sa validité, sa fiabilité, son admissibilité ou son efficacité.

- **Absence d'obligation de mener des consultations publiques.** Sauf pour le service policier de Toronto, il n'existe aucune obligation en Ontario de mener une consultation publique sur les systèmes d'IA utilisés dans le secteur pénal.

La CDO reconnait que la règlementation de l'IA dans le secteur pénal en est encore à ses débuts en Ontario et au Canada. La directive fédérale, l'EIA, la *LRSCN*, la directive de l'Ontario sur l'IA et les politiques de la CSPT en matière d'IA ont toutes été adoptées au cours des dernières années. Cela dit, les décideurs politiques canadiens et provinciaux sont loin derrière leurs homologues internationaux dans la mise en place d'outils de gouvernance pour faire face à cette technologie en rapide évolution.

Il n'est pas trop tôt pour se demander ce qui pourrait arriver si les gouvernements ne règlementaient pas les systèmes d'IA utilisés dans le secteur pénal. Il ne s'agit pas d'une question hypothétique. Les systèmes d'IA utilisés dans le secteur pénal sont employés dans d'autres juridictions depuis plusieurs années. Les décideurs politiques disposent donc d'un historique détaillé des risques et des préjudices bien documentés et largement médiatisés, notamment les suivants :

- Risque d'arrestation ou d'emprisonnement injustifié.
- Biais dans les données et discrimination.
- Absence de responsabilité juridique.
- Risques pour la vie privée, les droits de la personne et l'équité procédurale.
- Incohérence dans les pratiques policières et les décisions judiciaires.
- Perte de confiance du public dans le système de justice pénale.
- Risque d'aggraver la surreprésentation actuelle des communautés à faible revenu, racisées et autochtones dans le système de justice pénale.

À défaut de mesures proactives, ces risques et conséquences sont à la fois prévisibles et significatifs.

La CDO estime qu'il est urgent de garantir la fiabilité de l'IA dans le secteur pénal au Canada. L'intelligence artificielle dans le système judiciaire pénal soulève des questions cruciales pour la société canadienne, telles que la sécurité publique, les droits constitutionnels, les droits de la personne, les libertés civiles, la protection de la vie privée, l'équité procédurale et la confiance du public dans les institutions publiques clés, telles que les tribunaux et la police.

# 10. Prochaines étapes et coordonnées

L'une des leçons importantes tirées de ce projet est que l'incidence positive ou négative de l'IA dans le système de justice pénale repose sur une série complexe et interdépendante de choix techniques, opérationnels, politiques et juridiques. Une deuxième leçon importante est qu'il est essentiel de mettre en place des collaborations et des consultations à grande échelle. Compte tenu des enjeux, aucune organisation ou partie prenante ne peut ni ne doit agir de manière unilatérale.

La CDO est convaincue que les décideurs politiques provinciaux et les parties prenantes sont déterminés à traiter ces questions de manière réfléchie et collaborative. À cette fin, la CDO organisera des consultations sur le projet au cours des prochains mois.

Les personnes ou organisations intéressées par une collaboration avec la CDO sont invitées à contacter Ryan Fritsch, responsable du projet de la CDO sur l'IA dans le secteur de la justice pénale, à rfritsch@lco-cdo.org.

De plus amples renseignements sur nos projets de consultation, nos documents de réflexion sur l'IA dans le système de justice pénale et d'autres renseignements sont disponibles sur notre site Web.

Vous pouvez également contacter la CDO à :

Commission du droit de l'Ontario
2032, édifice Ignat Kaneff
Faculté de droit Osgoode Hall, Université York
4700, rue Keele, Toronto ON M3J 1P3

Tél. : 416 650-8406
Courriel : LawCommission@lco-cdo.org
Web : https://www.lco-cdo.org
LinkedIn : https://linkedin.com/company/lco-cdo
Bluesky : @lco-cdo.bsky.social
X : @LCO_CDO
YouTube : @lawcommissionofontario8724

# Annexe A
# Questions de consultation consolidées

Les questions suivantes reflètent les thèmes et les enjeux clés abordés dans les documents thématiques sur l'IA dans le système de justice pénale publiés par la CDO. Elles sont proposées à titre de points de départ pour la discussion et la consultation publiques. En plus de ces questions consolidées, les documents thématiques comprennent des questions détaillées sur les enjeux soulevés dans chaque document.

## 1. Normes provinciales

Les documents thématiques soulignent la nécessité d'adopter des règles provinciales établissant des règles et des critères clés en matière de fiabilité de l'IA dans le secteur de la justice pénale. Les documents thématiques proposent de nombreux modèles possibles, notamment :

- Législation ou règlementation fédérale (*Code criminel*, directive fédérale sur la PDA).
- Législation ou règlementation provinciale (*LRSCN*, législation policière, directive de l'Ontario sur l'IA).
- Politiques institutionnelles en matière de justice pénale (police, tribunaux, manuel des procureurs de la Couronne).

***Croyez-vous qu'un cadre provincial soit nécessaire? Si oui, quelle serait la meilleure approche et pour quelles raisons?***

## 2. Utilisations interdites et critères de risque

Le règlement de l'UE sur l'IA, la *LIAD* et la Politique sur l'IA de la Commission de services policiers de Toronto adoptent tous une forme de gouvernance de l'IA fondée sur les risques, qui comprend des utilisations présumées interdites ou des systèmes d'IA présumés « à haut risque » soumis à des exigences plus strictes et à une surveillance accrue.

***En principe, êtes-vous d'accord avec le cadre interdisant ou présentant un risque élevé? Quels critères devraient être adoptés pour identifier les systèmes interdits ou présentant un risque élevé? La législation canadienne fournit-elle des indications sur la manière dont les différents systèmes ou utilisations de l'IA devraient être classés?***

***Si vous estimez que certains systèmes ou certaines utilisations devraient être interdits ou identifiés comme « à haut risque » :***

- ***Quels systèmes ou utilisations de l'IA devraient entrer dans ces catégories?***
- ***Faut-il interdire la reconnaissance faciale en temps réel ou le maintien de l'ordre prédictif? Si oui, existe-t-il des exceptions raisonnables, telles que la reconnaissance faciale pour aider à retrouver des personnes disparues? Quelles règles devraient s'appliquer?***
- ***Quelles règles de surveillance ou exigences procédurales sont appropriées pour les systèmes à haut risque?***

## 3. Partialité, confidentialité et équité procédurale

Les initiatives en matière d'IA fiable dans le secteur de la justice pénale comprennent systématiquement des principes ou des règles détaillées visant à garantir que ces systèmes ne sont pas discriminatoires et protègent la vie privée et l'équité procédurale. Les composantes de ces initiatives varient, mais comprennent souvent les éléments suivants :

- Obligation de divulgation des systèmes d'IA dans le secteur pénal, y compris les « registres publics d'IA ».
- Interdiction des systèmes d'IA dans le secteur pénal présentant le niveau de risque le plus élevé.
- Critères permettant d'identifier les systèmes interdits ou à risque élevé.
- Limitations de la finalité et de l'utilisation.
- Évaluations obligatoires et transparentes de l'incidence de l'IA.
- Exigences en matière d'atténuation.
- Obligations obligatoires de mesurer, de corriger et de contrôler les biais dans les systèmes d'IA.
- Garanties procédurales, telles que l'obligation d'obtenir un mandat pour les systèmes à risque élevé.
- Exigences obligatoires en matière d'intervention humaine et d'apprentissage.
- Exigences obligatoires en matière d'audit et d'évaluation.

Les documents thématiques soulignent également que les variations au sein des systèmes d'IA dans le secteur pénal et entre eux ont des conséquences importantes pour leurs risques et leurs effets sur les droits.

***En principe, êtes-vous d'accord pour que la province et les institutions de justice pénale de l'Ontario s'engagent explicitement à garantir que les systèmes d'IA utilisés dans le secteur pénal ne soient pas discriminatoires, protègent le droit à la vie privée et puissent être expliqués?***

***À votre avis, lesquels des éléments énumérés ci-dessus sont nécessaires pour garantir que les systèmes d'IA dans le secteur pénal protègent les droits? La législation canadienne indique-t-elle quels éléments devraient être adoptés?***

***Quelle est la meilleure façon d'évaluer l'incidence des différents systèmes d'IA dans le secteur pénal sur les droits? Faut-il prévoir une échelle mobile des exigences en matière d'atténuation en fonction du risque présenté par le système?***

## 4. Divulgation

La divulgation est un thème récurrent dans les législations et les cadres règlementaires relatifs à la fiabilité de l'IA dans le système de justice pénale. Il existe plusieurs options quant au moment, à la forme et au contenu des obligations de divulgation.

***Comment et dans quelle mesure les systèmes d'IA dans le secteur pénal doivent-ils être divulgués?***

***Faut-il mettre en place un registre obligatoire ou un rapport public sur l'IA? Si oui, devraient-ils contenir :***

- ***Une analyse d'incidence détaillée ou sommaire?***
- ***Une description complète ou sommaire des données d'apprentissage?***
- ***Des données de sortie pour faciliter l'audit indépendant, la supervision et le suivi des performances?***

***Comment promouvoir la divulgation tout en protégeant d'autres objectifs légitimes, tels que la confidentialité des enquêtes?***

## 5. Évaluations de l'incidence

La nécessité de réaliser des analyses de l'incidence est un thème récurrent dans la législation et les cadres relatifs à l'IA dans le système de justice pénale. Plusieurs choix s'offrent en ce qui concerne le moment, la forme et le contenu des analyses d'incidence.

- ***La province devrait-elle exiger une évaluation obligatoire de l'incidence des systèmes d'IA dans le secteur pénal en Ontario? Êtes-vous d'accord pour qu'une évaluation de l'incidence porte sur la vie privée, les droits de la personne et l'équité procédurale, et qu'elle fournisse des garanties quant à la manière dont un système d'IA se conformera à d'autres obligations légales?***
- ***Quels autres renseignements ou risques devraient être inclus?***
- ***Comment garantir que les analyses de l'incidence sont utilisées et communiquées de manière cohérente?***

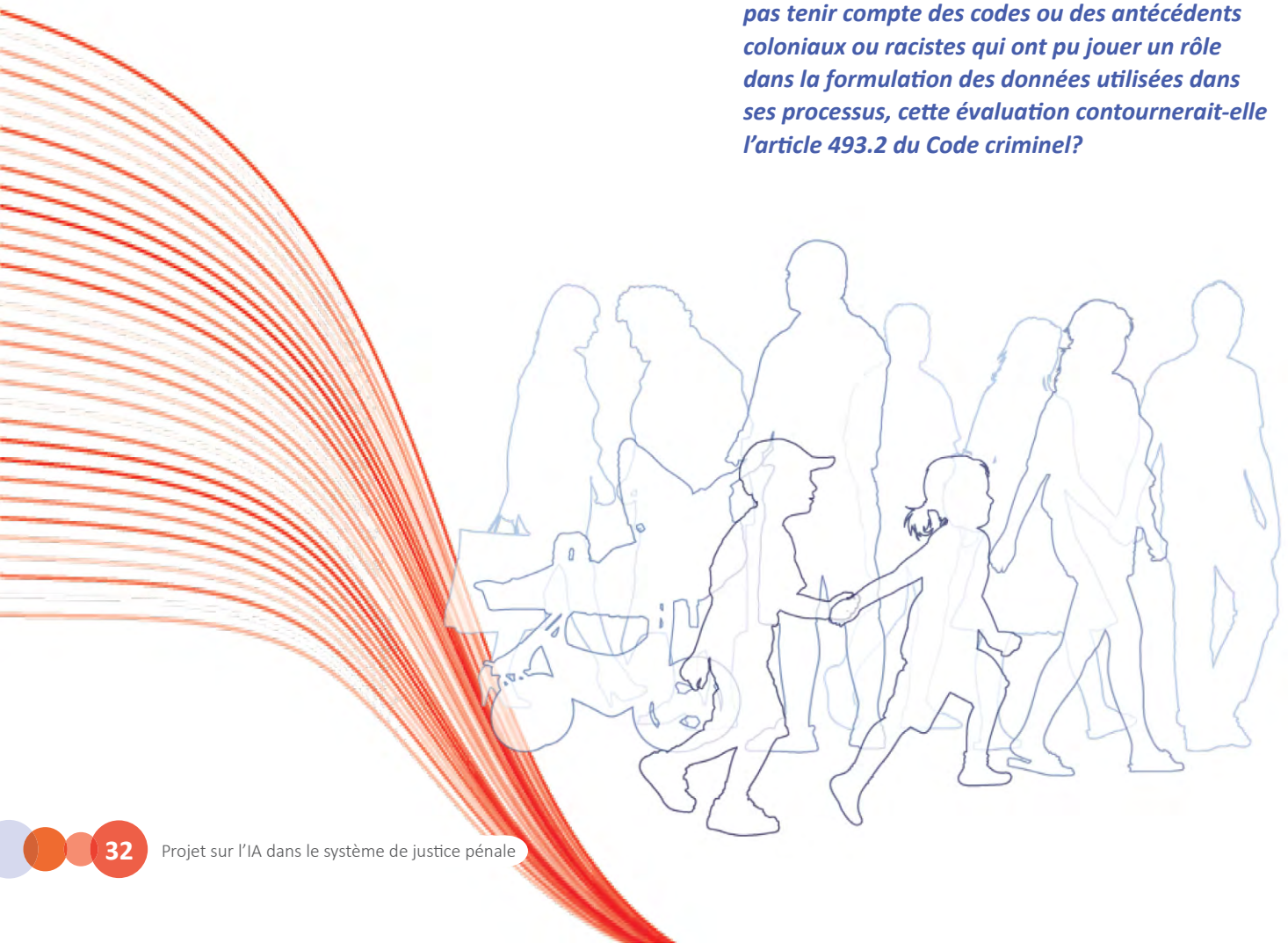
## 6. Évaluation des risques liés à la mise en liberté sous caution et à la détermination des peines

L'évaluation du risque lié à la mise en liberté sous caution et à la détermination des peines par l'IA et les algorithmes soulèvent de nombreux défis, notamment des questions relatives aux préjugés et à la discrimination, à la divulgation et à la capacité d'un accusé à contester les prédictions d'un algorithme.

***Comment le système juridique peut-il garantir que les scores de risque générés par l'IA respectent les normes d'ouverture, de transparence et de fiabilité nécessaires pour protéger les droits des personnes et préserver l'intégrité du processus judiciaire?***

***Les évaluations des risques par l'IA, qui produisent des résultats basés sur des données discriminatoires, ont-elles leur place dans la détermination des peines des délinquants autochtones et noirs?***

***Si une évaluation des risques par l'IA ne peut pas tenir compte des codes ou des antécédents coloniaux ou racistes qui ont pu jouer un rôle dans la formulation des données utilisées dans ses processus, cette évaluation contournerait-elle l'article 493.2 du Code criminel?***



## 7. Litiges liés à l'IA

Les documents thématiques examinent comment les systèmes d'IA dans le secteur pénal soulèvent de nouveaux défis complexes en matière de procédure, de preuve et de contentieux, notamment :

- L'admissibilité et la fiabilité des preuves issues de l'IA et la question de savoir si l'IA constitue une « preuve d'expert ».
- L'utilisation de l'IA pour générer des rapports d'incident, résumer ou analyser les données des caméras corporelles, etc.
- Les observations à la cour assistées par l'IA ou les résumés de divulgation.
- Les preuves hypertruquées.
- Les déclarations de témoins générées par l'IA, les déclarations des victimes, les rapports *Gladue*, etc.
- Les litiges relatifs aux allégations de « secrets commerciaux » ou de « secret professionnel des enquêteurs ».
- Les mandats ou les demandes *O'Connor* pour obtenir des preuves provenant de tiers.

***Comment pouvons-nous règlementer, formaliser ou rationaliser les questions fréquemment litigieuses liées à l'IA telles que celles mentionnées ci-dessus?***

***Une exigence systématique de divulgation complète d'un système d'IA et de ses composants serait-elle atténuée par des mesures objectives de performance de l'IA, telles que des audits techniques indépendants qui en valident la fiabilité et la performance?***

***Avons-nous besoin de normes ou de pratiques régissant les déclarations ou rapports générés par l'IA afin d'en garantir la fiabilité et l'admissibilité?***

## 8. Engagement public

De nombreux systèmes d'IA utilisés dans le secteur pénal ont été critiqués par des communautés qui estiment ne pas avoir été consultées ni informées au sujet de systèmes qui les concernent. De nombreuses initiatives en matière de fiabilité de l'IA dans le secteur de la justice pénale, notamment la politique du service de police de Toronto en matière d'IA, prévoient des exigences en matière d'engagement du public.

***Comment le public devrait-il être impliqué dans l'élaboration, l'évaluation ou la surveillance des politiques en matière d'IA dans le système de justice pénale?***

## 9. Accès à la justice

Les documents thématiques comprenaient des discussions approfondies sur l'incidence systémique potentielle des systèmes d'IA dans le secteur pénal sur l'accès à la justice et les communautés racisées, autochtones ou à faible revenu en Ontario.

***Outre les mesures évoquées ci-dessus, comment le système de justice pénale de l'Ontario peut-il garantir l'accès à la justice si les systèmes d'IA dans le secteur pénal sont largement adoptés dans la province?***

***Quelles politiques ou mesures de soutien sont nécessaires pour garantir l'accès à la justice aux personnes accusées d'infractions criminelles qui n'ont pas les moyens de contester les systèmes d'IA utilisés dans le secteur pénal?***

## 10. Capacité institutionnelle

Les documents thématiques examinent comment les systèmes d'IA dans le secteur pénal posent de nouveaux défis aux institutions de justice pénale de l'Ontario.

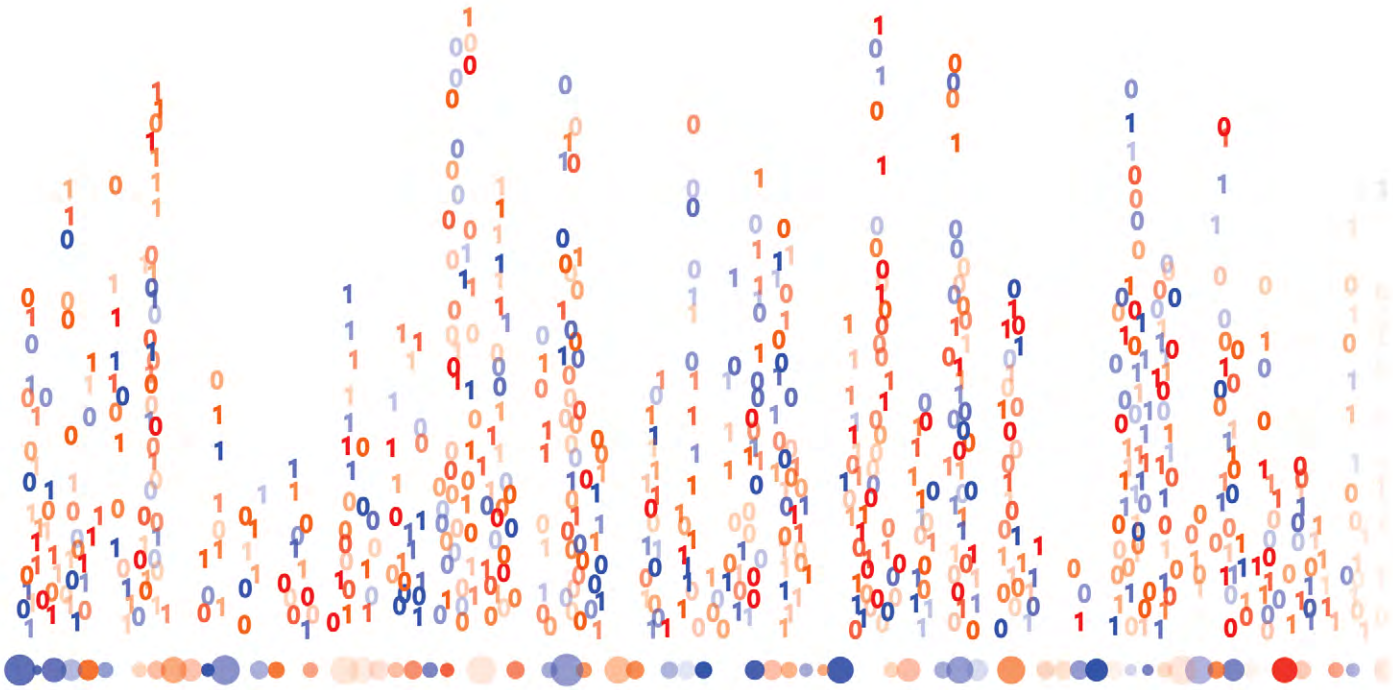
***Le système judiciaire provincial a-t-il la capacité de relever ces défis? Si ce n'est pas le cas, quels outils ou soutiens sont nécessaires pour aider les institutions à relever ces défis de manière proactive?***

## 11. Surveillance systémique

Outre les mesures évoquées ci-dessus, nombreux sont ceux qui estiment nécessaire de mettre en place un contrôle indépendant des systèmes d'IA utilisés dans le secteur public, y compris dans le système de justice pénale.

***Étant donné que de nombreuses institutions de justice pénale font l'objet ou sont soumises à des formes de contrôle, comment fonctionnerait le contrôle de l'IA?***

***L'Ontario a-t-il besoin d'un nouvel organisme de surveillance indépendant ou cette fonction peut-elle être intégrée aux organismes existants?***



# Notes

1 Le maintien de l'ordre prédictif est abordé dans le document de travail n° 2 du projet de la CDO sur l'IA dans le système de justice pénale, intitulé « Utilisation de l'IA par les forces de l'ordre » [document de travail de la CDO sur l'IA dans le domaine policier], rédigé par Ryan Fritsch, conseiller en politiques de la CDO. Ce rapport est disponible en ligne au https://www.lco-cdo.org/fr/nos-projets-en-cours/lia-dans-le-systeme-de-justice-penale/. Voir aussi, Andrew Guthrie Ferguson, « Predictive Policing Theory » publié comme chapitre 24 dans Tamara Rice Lave et Eric J. Miller (éd.), The Cambridge Handbook of Policing in the United States [Ferguson 2019] (2019), en ligne : https://ssrn.com/abstract=3516382; National Academies of Sciences, Engineering, and Medicine, Law Enforcement Use of Predictive Policing Approaches: Proceedings of a Workshop – In Brief [NAS Predictive Policing] (2024), en ligne : https://nap.nationalacademies.org/catalog/28037/law-enforcement-use-of-predictive-policing-approaches-proceedings-of-a; et The Citizen Lab, To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada [To Surveil and Protect] (2020), en ligne : https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf.

2 Ferguson 2019 p. 491.

3 To Surveil and Protect p. 41-46.

4 Voir de manière générale, document thématique sur l'utilisation de l'IA par la police de la CDO et NAS Predictive Policing, p. 3-4.

5 To Surveil and Protect p. 47.

6 Les technologies de reconnaissance faciale utilisées par la police sont abordées dans le document thématique de la CDO sur l'IA dans les forces de l'ordre. Voir également, de manière générale, Organisation internationale de police criminelle (INTERPOL), A Policy Framework for Responsible Limits on Facial Recognition [Cadre stratégique d'INTERPOL] (2021), en ligne : https://unicri.org/A-Policy-Framework%20-for-Responsible-Limits-on-Facial-Recognition; International Network of Civil Liberties Organizations, Eyes on the Watchers: Challenging the Rise of Police Facial Recognition Technology [INCLO Challenging FRT] (2025), en ligne: https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/; et Commissaire à l'information et à la protection de la vie privée de l'Ontario, La reconnaissance faciale et les bases de données de photos signalétiques : document d'orientation à l'intention des services de police de l'Ontario [Rapport de la CIPVP sur la RF] (2024), en ligne : https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-la-reconnaissance-faciale-et-les-bases-de-donnees-de-photos-signaletiques-document-d-orientation-a-l-intention-des-services-de-police-en-ontario-f.pdf.

7 Rapport de la CIPVP sur la RF p. 1.

8 Organisation internationale de police criminelle (INTERPOL), Introduction to Responsible AI Innovation (2024) [INTERPOL AI Introduction], en ligne : https://www.interpol.int/fr/Notre-action/Innovation/Manuel-d-utilisation-de-l-intelligence-artificielle p. 21.

9 Europol, AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement [EUROPOL] (2024), en ligne : https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing p. 21-29.

10 Par exemple voir United States Government Accountability Office, Report to Congressional Requesters, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks (2021), en ligne : https://www.gao.gov/assets/gao-21-518.pdf.

11 Commissariat à la protection de la vie privée du Canada, Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de l'Alberta [Enquête conjointe sur Clearview AI] (2 février 2021), en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2021/lprpde-2021-001/.

12 Services policiers de Toronto, Update on the Implementation of the Board's Policy on the Use of AI Technology (11 janvier 2024), en ligne : https://tpsb.ca/jdownloads-categories?task=download.send&id=813:january-11-2024-public-agenda&catid=32.

13 Les systèmes d'IA associés à la mise en liberté sous caution et à la détermination des peines font l'objet du rapport no 3 de la CDO sur l'IA dans le système de justice pénale, L'IA et l'évaluation du risque associé à la mise en liberté sous caution, à la détermination des peines et à la récidive par Armando D'Andrea, responsable du comité pénal et ancien avocat de service en matière criminelle, Aide juridique Ontario et Gideon Christian, faculté de droit, Université de Calgary. Ce rapport est disponible en ligne au https://www.lco-cdo.org/fr/nos-projets-en-cours/lia-dans-le-systeme-de-justice-penale/. Voir également Commission du droit de l'Ontario, The Rise and Fall of Algorithms in American Criminal Justice : Lessons for Canada [LCO American Lessons] (2020) [document thématique de la CDO sur l'AI dans le système de justice pénale], en ligne : https://www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28-2020.pdf.

14 The Champion, Making Sense of Risk Assessments, American National Association of Criminal Defense Lawyers, [The Champion] (2018), en ligne : https://www.nacdl.org/Article/June2018-MakingSenseofPretrialRiskAsses. Voir également LCO American Lessons.

15 Sarah Picard-Fritshe et al, Center on Court Innovation, Beyond the Algorithm: Pretrial Reform, Risk Assessment, and Racial Fairness (2019), en ligne :

https://www.courtinnovation.org/sites/default/files/media/document/2019/Beyond_The_Algorithm.pdf p. 3.

16 Ces systèmes sont décrits dans plusieurs documents relatifs au projet de la CDO sur l'IA dans le système de justice pénale, notamment le rapport no 1, Introduction au projet sur l'IA dans le système de justice pénale de la CDO [LCO Criminal AI Introduction] par le directeur général de la CDO Nye Thomas; rapport no 2 L'utilisation de l'IA par les forces de l'ordre; et rapport no 4, L'IA durant le procès et en appel, par Paula Thompson, Initiatives stratégiques, ministère du Procureur général, et Eric Neubauer, avocat de la défense, Neubauer Law, et coprésident, Criminal Lawyers Association Technology Committee. Ces rapports sont disponibles en ligne au https://www.lco-cdo.org/fr/nos-projets-en-cours/lia-dans-le-systeme-de-justice-penale/.

17 Pour une discussion approfondie sur les biais dans les données d'IA, voir American Lessons par la CDO p. 20-26. Pour une analyse détaillée de l'IA et des droits de la personne en général, voir Commission du droit de l'Ontario, Accountable AI, (2022) [Accountable AI], en ligne : https://www.lco-cdo.org/fr/nos-projets-en-cours/intelligence-artificielle-pda-et-systeme-de-justice/reglementer-lintelligence-artificielle-enjeux-et-choix-essentiels/ p. 40-55. La CDO et la Commission ontarienne des droits de la personne ont également récemment élaboré la première évaluation de l'incidence de l'IA sur les droits de la personne (EIDP) fondée sur le droit canadien. L'EIDP de la CDO et de la CODP et un document d'information complémentaire sont disponibles au https://www.lco-cdo.org/fr/nos-projets-en-cours/intelligence-artificielle-pda-et-systeme-de-justice/evaluation-de-limpact-de-lintelligence-artificielle-sur-les-droits-de-la-personne/.

18 INCLO Challenging FRT p. 25. L'étude la plus connue sur les biais de la RF est un rapport publié en 2019 par le National Institute of Standards and Technology, qui a révélé que « la majorité des systèmes commerciaux de reconnaissance faciale présentent des biais » et « identifient à tort les visages afro-américains et asiatiques 10 à 100 fois plus souvent que les visages caucasiens ». National Institute of Standards and Technology (NIST), Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (2019), en ligne : https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf p. 3. Le NIST également identifié des préoccupations concernant les faux négatifs, les faux positifs, le genre et l'âge.

19 NAS Predictive Policing p. 2 : « dans la pratique, les algorithmes prédictifs favorisent la surveillance policière dans les zones sensibles, ce qui conduit trop souvent à une surveillance excessive des communautés et des habitants, imposant des préjugés néfastes pour les personnes de couleur. » Voir également, Partnership on AI (PAI), Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System, (avril 2019), en ligne : https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/.

20 Voir par exemple, Policing Project, New York University School of Law, Law Enforcement Use of Facial Recognition Technology Must Be Regulated Now. Here's How [Policing Project FRT Regulation] (consulté en mars 2025), en ligne : https://www.policingproject.org/regulating-police-use-of-face-recognition-technology at 1-2; Surveillance Technology Oversight Project (STOP), Seeing Is Misbelieving: How Surveillance Technology Distorts Crime Statistics (juin 2024), en ligne : https://www.stopspying.org/seeing-is-misbelieving; cadre stratégique d'INTERPOL; et INCLO Challenging FRT.

21 Voir de manière générale, Cadre stratégique d'INTERPOL et INCLO Challenging FRT à titre d'exemple.

22 Brennan Center for Justice, New York University School of Law, New York City Police Department Surveillance Technology (2019), en ligne : https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

23 Par exemple, voir Cadre stratégique d'INTERPOL p. 15-16. Voir également Commissaire à l'information et à la protection de la vie privée de l'Ontario, La reconnaissance faciale et les bases de données de photos signalétiques : document d'orientation à l'intention des services de police de l'Ontario [Orientation sur les photos signalétiques] (janvier 2024), en ligne : https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-la-reconnaissance-faciale-et-les-bases-de-donnees-de-photos-signaletiques-document-d-orientation-a-l-intention-des-services-de-police-en-ontario-f.pdf. Ce rapport présente des directives détaillées sur les questions liées à la mise en œuvre de la RF, les considérations opérationnelles, ainsi que l'examen et l'évaluation de programmes, p. 4-33.

24 Voir le rapport de la CDO American Lessons pour un bon résumé de ces questions.

25 Enquête conjointe sur Clearview AI.

26 David Freeman Engstrom et Daniel E. Ho, « Algorithmic Accountability in the Administrative State » dans (2020) Yale Journal on Regulation 800, en ligne : papers.ssrn.com/sol3/papers.cfm?abstract_id= 3965041 p. 821.

27 Voir INCLO Challenging FRT, Ferguson 2019, et le rapport de la CDO American Lessons pour des exemples représentatifs de cette analyse.

28 Les variations entre les systèmes d'IA dans le secteur de la justice pénale et au sein même de ces systèmes confirment la nécessité de disposer d'outils et de critères permettant d'évaluer systématiquement les avantages et les risques de l'IA. Par exemple, un système de reconnaissance faciale surveillant une manifestation publique présente des risques plus graves pour la Charte et la vie privée qu'un système de reconnaissance faciale surveillant une installation fermée et sécurisée. Les systèmes de maintien de l'ordre prédictif peuvent également varier considérablement en termes de portée et de risque : les systèmes basés sur la géolocalisation ont été utilisés pour gérer les patrouilles de police, pour identifier les moments et les lieux où des crimes spécifiques sont susceptibles de se produire, et pour cerner les zones où des interventions communautaires pourraient réduire la criminalité. Les systèmes basés sur les personnes, en revanche, ont été utilisés pour prédire les individus les plus susceptibles d'être impliqués dans des crimes, pour promouvoir la sécurité des agents lorsqu'ils répondent à des appels d'urgence, et pour promouvoir une « dissuasion ciblée ».

29 NAS Predictive Policing p. 1.

30 Ces rapports sont documentés de manière exhaustive dans chacun des documents thématiques du projet de la CDO sur l'IA dans le système de justice pénale.

31 Union européenne, règlement (UE) 2024/1689 du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle [règlement de l'UE sur l'IA] (2024), en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32024R1689. Le chapitre II, article 5 du règlement de l'UE sur l'IA énonce plusieurs « risques inacceptables » et interdictions relativement à certains systèmes d'IA. Ces systèmes sont réputés « inacceptables » parce qu'ils constituent une menace évidente pour les valeurs européennes et les droits fondamentaux. L'article 5 interdit deux systèmes d'IA qui portent directement sur la justice pénale :
1. *L'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins autres que répressives.*
*2. L'évaluation du risque qu'une personne commette des infractions pénales sur la seule base d'un profilage ou de traits de personnalité.*
Ces deux interdictions font l'objet d'exceptions importantes.

32 Dans le règlement de l'UE sur l'IA, le chapitre III, annexe III énumère des systèmes « à haut risque » comme :
*Autorités répressives*
• *Utilisés pour évaluer le risque qu'une personne ne devienne victime d'infractions pénales.*
• *Les polygraphes.*
• *Pour évaluer la fiabilité des preuves dans le cadre d'enquêtes ou de poursuites relatives à des infractions pénales.*
• *Évaluer le risque d'infraction ou de récidive d'une personne physique non seulement sur la base du profilage ou sur la base de l'évaluation des traits de personnalité ou d'antécédents judiciaires.*
*Administration de la justice*
*Les systèmes d'IA destinés à être utilisés dans la recherche et l'interprétation des faits et à appliquer la loi à un ensemble concret de faits ou utilisés pour le règlement extrajudiciaire des litiges.*

33 Les initiatives américaines sont discutées en détail dans l'introduction au projet de la CDO sur l'IA dans le système de justice pénale. Voir aussi de manière générale, États-Unis, Bureau du président, décret présidentiel 14110 « Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence » (1er novembre 2023), en ligne : https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence; Bureau de la gestion et du budget, décret exécutif M-24-10 « Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence » (mars 2023); AINow Institute, "A Taxonomy of Legislative Approaches to Face Recognition in the United States" in Regulating Biometrics: Global Approaches and Open Questions (sept. 2020), en ligne: https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions; New York Police Department, Facial Recognition Technology Policy, P.G. 212-129, (2020), en ligne: https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page; et Policing Project, New York University School of Law, Regulating Police Use of Facial Recognition Technology – Resources for Legislators (consulté en mars 2025), en ligne: https://www.policingproject.org/regulating-police-use-of-face-recognition-technology.

34 Loi sur la mise en œuvre de la Charte du numérique; 1re sess. 44e législature, 2022, partie 3 « Loi sur l'intelligence artificielle et les données » [LIAD], en ligne : https://www.parl.ca/legisinfo/fr/projet-de-loi/44-1/c-27.

35 LIAD, art. 3.

36 Voir par exemple, une lettre ouverte conjointe de 45 organisations civiles, experts et universitaires critiquant la LIAD pour de nombreuses raisons, en ligne : https://bccla.org/policy-submission/joint-letter-of-concern-regarding-the-artificial-intelligence-and-data-act-aida/.

37 Canada. Innovation, Sciences et Développement économique Canada, « Lettre au président du Comité permanent de l'industrie et de la technologie sur le projet de loi C-27 » (28 novembre 2023), en ligne : https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-f.pdf. Les classes de systèmes interdits concernées comprennent la classe 3 (« utilisation d'un système d'intelligence artificielle pour traiter des données biométriques…), la classe 6 (« utilisation d'un système d'intelligence artificielle par un tribunal ou un organisme administratif…) et la classe 7 (« utilisation d'un système d'intelligence artificielle pour assister un agent de la paix…).

38 Voir par exemple, Conseil du Canada de l'accès et la vie privée, « Key stakeholders call for withdrawal of controversial AI legislation » 24 avril 2024, en ligne : https://pacc-ccap.ca/aida-open-letter/.

39 Canada, Directive sur la prise de décisions automatisée [Canada Directive sur la PDA] (2019), en ligne : https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32592; et Outil d'évaluation de l'incidence algorithmique [Canada EIA], en ligne : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai/evaluation-incidence-algorithmique.html.

40 Accountable AI.

41 Voir Accountable AI p. 57-66.

42 Canada Directive sur la PDA, art. 5.1. Il est à noter que la directive s'applique uniquement aux ministères fédéraux relevant du Secrétariat du Conseil du Trésor.

43 Cet examen devrait être achevé en 2025.

44 La création du PNIT est abordée dans Gendarmerie royale du Canada, « La GRC publie le Plan de transparence : Aperçu des technologies opérationnelles » [Plan de transparence GRC] (septembre 2024), en ligne : https://grc.ca/fr/nouvelles/2024/09/grc-publie-plan-transparence-apercu-technologies-operationnelles

45 Communication de la GRC avec la CDO.

46 Gendarmerie royale du Canada, Programme national d'intégration de la technologie de la GRC – Plan de transparence : Aperçu des technologies opérationnelles [Plan de transparence GRC] (2024), en ligne au https://grc.ca/fr/renseignements-organisationnels/publications-et-guides/programme-national-dintegration-technologie-plan-de-transparence.

47 Plan de transparence GRC p. 9.

48 Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique, L.O. 2024, chap. 24, en ligne : https://www.ontario.ca/lois/loi/24e24.

49 Gouvernement de l'Ontario, Consultation sur les projets de loi : Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public (2024), en ligne : https://www.ontariocanada.com/registry/view.do?language=fr&postingId=47433.

50 Commission du droit de l'Ontario, Projet de loi 194, mémoire de la Commission du droit de l'Ontario [mémoire de la CDO sur le projet de loi 194] (2024), en ligne : https://www.lco-cdo.org/en/lco-releases-bill-194-submission/.

51 Le paragraphe 5 (1) de la Loi visant à renforcer la sécurité et la confiance en matière de numérique prévoit que ses dispositions concernant les systèmes d'IA « s'appliquent aux entités du secteur public prescrites si elles utilisent ou prévoient utiliser un système d'intelligence artificielle dans des circonstances prescrites ». Cet article inclut deux limites importantes.
D'abord, le paragraphe 1 (1) définit les « entités du secteur public » qui seront assujetties à la *Loi*, y compris :
*a) une institution, autre que l'Assemblée, au sens du paragraphe 2 (1) de la Loi sur l'accès à l'information et la protection de la vie privée;*
*b) une institution au sens du paragraphe 2 (1) de la Loi sur l'accès à l'information municipale et la protection de la vie privée;*
*c) une société d'aide à l'enfance;*
*d) un conseil scolaire. (« public sector entity »).*
[Italique ajouté.] à noter que ni le paragraphe 2 (1) de la *Loi sur l'accès à l'information et la protection de la vie privée* ni le paragraphe 2 (1) de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* n'inclut les services policiers, les cours ou les tribunaux administratifs. En conséquence, ces institutions ne sont pas soumises à la gouvernance ni aux exigences de la *LRSCN*.
Ensuite, le par. 5 (1) permet à la province de prescrire les « utilisations » ou les « circonstances » de l'IA qui sont assujetties à la législation. Ni le terme « utilisation » ni le terme « circonstances » ne sont définis dans la *LRSCN*.

52 Gouvernement de l'Ontario, ministère des Services au public et aux entreprises et de l'Approvisionnement, Directive sur l'utilisation responsable de l'intelligence artificielle, 1er décembre 2024 [Directive de l'Ontario sur l'IA].

53 La Directive de l'Ontario sur l'IA est abordée en détail dans Introduction au projet de la CDO sur l'IA dans le système de justice pénale.

54 Commission de services policiers de Toronto, Use of Artificial Intelligence Technology [Politique de la CSPT sur l'IA] (28 février 2022 ; mis à jour le 11 janvier 2024), en ligne : https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

55 Politique de la CSPT sur l'IA, « Guiding Principles ».

56 Idem.

57 Politique de la CSPT sur l'IA, « Policy of the Board ».

58 Services policiers de Toronto, Update on the Implementation of the Board's Policy on the Use of AI Technology (11 janvier 2024), en ligne : https://tpsb.ca/jdownloads-categories?task=download.send&id=813:january-11-2024-public-agenda&catid=32.

59 Conseil des services de la police régionale de Durham, Use of Artificial Intelligence Policy, octobre 2024, en ligne au https://durhampoliceboard.ca/policies-and-bylaws/.

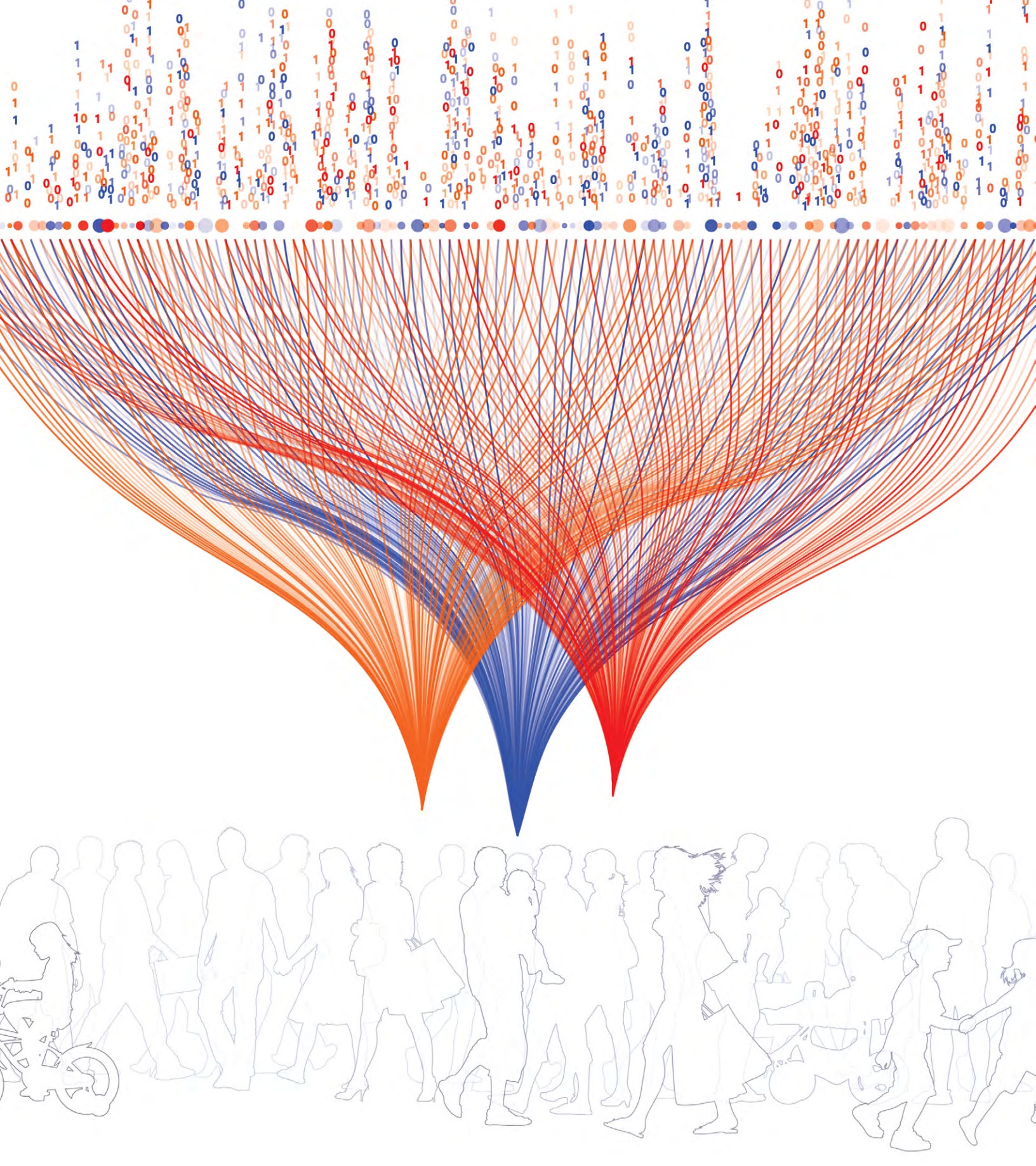
60 La Commission ontarienne des droits de la personne et la Commissaire à l'information et à la protection de la vie privée de l'Ontario ont récemment critiqué la CSPT pour avoir classé leur utilisation de certaines technologies d'IA – y compris les lecteurs automatiques de plaques d'immatriculation et l'identification par empreintes digitales – comme des « technologies à faible risque » soumises à moins d'exigences en matière d'évaluation et de surveillance. Commissaire à l'information et à la protection de la vie privée de l'Ontario, « Letter to the Toronto Police Services re AI Policy and Risk Classification Report » (10 janvier 2024), en ligne : https://www.ipc.on.ca/resource/letter-to-the-toronto-police-services-board-about-facial-recognition-mugshot-database-program/; et Commission ontarienne des droits de la personne, « Approbation des technologies à haut risque dans le cadre de la politique de la Commission des services policiers de Toronto sur l'utilisation des technologies d'intelligence artificielle » (10 janvier 2024) en ligne : https://www.ohrc.on.ca/fr/centre-des-nouvelles/approbation-des-technologies-haut-risque-dans-le-cadre-de-la-politique-de-la.

61 Ces rapports comprennent : Commissariat à la protection de la vie privée du Canada, Technologie de reconnaissance faciale : utilisation par les services de police au Canada et approche proposée (10 juin 2021), en ligne : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202021/sr_grc/; Enquête conjointe sur Clearview AI, Inc. par le Commissariat à la protection de la vie privée du Canada, déclaration conjointe, Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale (mai 2022), en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/surveillance/police-et-securite-publique/gd_rf_202205/; OPC Police FRT Guidance (2022); IPC Mugshot Guidance (2024); et Commissaire à l'information et à la protection de la vie privée de l'Ontario, Document d'orientation sur l'utilisation de systèmes de reconnaissance des plaques d'immatriculation par les services de police [IPC ALPR Guidance] (mis à jour en décembre 2024), en ligne : https://www.ipc.on.ca/fr/ressources/document-dorientation-sur-lutilisation-de-systemes-de-reconnaissance-des-plaques-dimmatriculation.

62 Cour fédérale du Canada, « Principes et lignes directrices intérimaires de la Cour sur son utilisation de l'intelligence artificielle » (20 décembre 2023) [Directive de pratique de la Cour fédérale], en ligne : https://www.fct-cf.ca/fr/pages/droit-et-trousse-doutils/intelligence-artificielle; et Cour fédérale du Canada, « Avis aux parties et à la communauté juridique : L'utilisation de l'intelligence artificielle dans les procédures judiciaires » (20 décembre 2023), en ligne : https://www.fct-cf.ca/Content/assets/pdf/base/2023-12-20-avis-utilisation-ia-procedures-judiciairess.pdf

63 Alberta, « Notice to the Profession & Public- Ensuring the integrity of court submissions when using Large Language Models » (octobre 2023), en ligne : https://www.albertacourts.ca/kb/resources/announcements/notice-to-the-profession-public---use-of-ai-in-citations-submissions; Manitoba, « Re : Use Of Artificial Intelligence In Court Submissions (juin 2023), en ligne : https://www.manitobacourts.mb.ca/site/assets/files/2045/practice_direction_-_use_of_artificial_intelligence_in_court_submissions.pdf; Québec, « L'intégrité des observations présentées aux tribunaux en cas d'utilisation des grands modèles de langage » (octobre 2023) en ligne : https://coursuperieureduquebec.ca/fileadmin/cour-superieure/Districts_judiciaires/Division_Montreal/Communiques/Avis_a_la_communaute_juridique-Utilisation_intelligence_artificielle_FR_-_24_octobre_2023.pdf.

64 Conseil canadien de la magistrature, Lignes directrices sur l'utilisation de l'intelligence artificielle dans les tribunaux canadiens (sept. 2024) [Lignes directrices du CCM], en ligne au https://cjc-ccm.ca/fr/nouvelles/le-conseil-canadien-de-la-magistrature-publie-des-lignes-directrices-sur-lutilisation-de.



LCO CDO
LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

2032 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, Ontario, Canada M3J 1P3