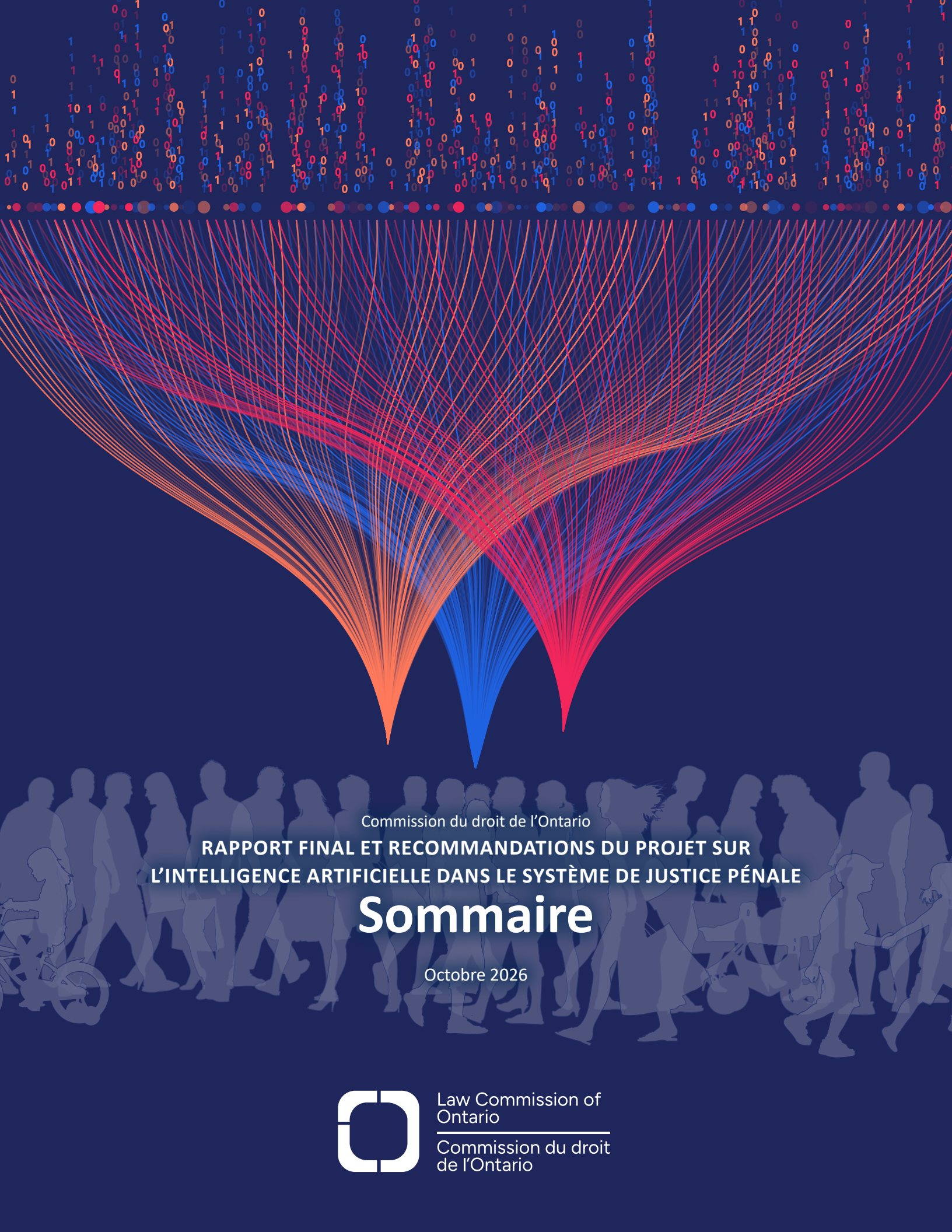




Commission du droit de l'Ontario

**RAPPORT FINAL ET RECOMMANDATIONS DU PROJET SUR
L'INTELLIGENCE ARTIFICIELLE DANS LE SYSTÈME DE JUSTICE PÉNALE**

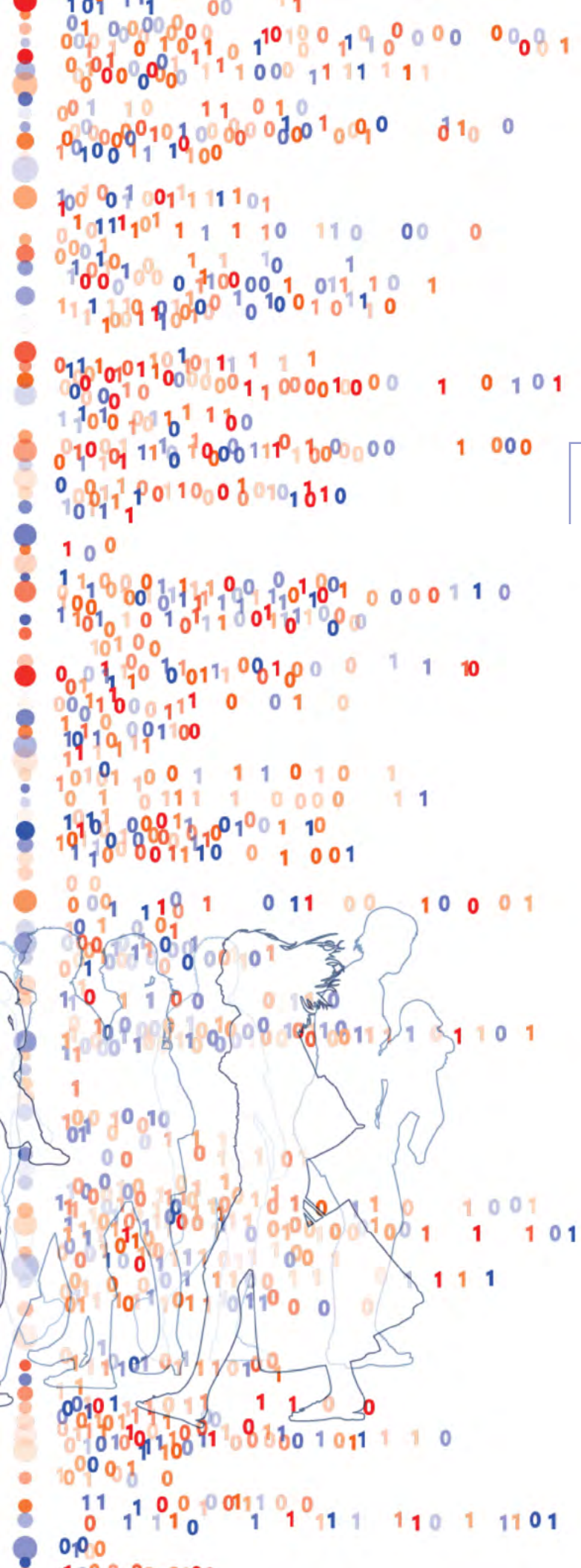
Sommaire

Octobre 2026



Law Commission of
Ontario

Commission du droit
de l'Ontario

The background of the page features a decorative design. On the left side, there is a vertical column of colored dots in shades of orange, blue, and red. The rest of the background is filled with a pattern of binary code (0s and 1s) in the same color palette. Overlaid on the bottom left of the page is a faint, light blue outline map of the province of 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 complexes et importantes de politique juridique. Par le biais de ses travaux, la CDO favorise l'accès à la justice, l'élaboration de lois et de politiques juridiques fondées sur des données probantes, ainsi que le débat public sur des enjeux actuels et importants en matière de réforme du droit.

Un conseil de gouverneurs, composé d'un large éventail de dirigeants du milieu juridique ontarien, guide les travaux de la CDO. La CDO reçoit du financement de la Fondation du droit de l'Ontario, du Barreau de l'Ontario et de la faculté de droit Osgoode Hall.

Pour en savoir plus sur la CDO et ce projet, consultez le site <https://lco-cdo.org/fr/>.



Law Commission of
Ontario

Commission du droit
de l'Ontario

Auteurs

Ryan Fritsch, avocat, Commission du droit de l'Ontario
Nye Thomas, directeur général, Commission du droit de l'Ontario

Non-responsabilité

L'analyse et les recommandations exprimées dans ce document ne reflètent pas nécessairement les opinions des bailleurs de fonds, des contributeurs, des membres du comité consultatif ou des auteurs des documents de travail de la CDO.

Responsable du projet et coordonnées

Le projet de la CDO sur l'IA dans le système de justice pénale est dirigé par Ryan Fritsch. On peut le joindre à rfritsch@lco-cdo.org et joindre la CDO aux adresses suivantes :

Commission du droit de l'Ontario
2030, édifice Ignat Kaneff
Faculté de droit Osgoode Hall, Université York
4700, rue Keele, Toronto ON Canada M3J 1P3

Tél. : 416 650-8406

Courriel : LawCommission@lco-cdo.org

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

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

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

Bailleurs de fonds

La CDO est financée par la Fondation du droit de l'Ontario, le Barreau de l'Ontario et la faculté de droit Osgoode Hall. La CDO tient à remercier la Commission du droit du Canada pour le financement accordé en vue de l'organisation des tables rondes de consultation à Vancouver et à Toronto.



Law Commission of Canada
Commission du droit du Canada

Le projet sur l'IA dans le système de justice pénale

Le [projet de la CDO sur l'IA dans le système de justice pénale](#) constitue la première étude exhaustive des opportunités, des risques et des enjeux liés à la réforme législative concernant l'IA dans le système canadien de justice pénale.

En avril 2025, la CDO a publié l'introduction du projet et quatre documents thématiques. Chaque document thématique examinait le recours à l'IA à un stade distinct du processus de justice pénale :

- [Rapport 1 : Introduction et sommaire](#)
- [Rapport 2 : L'utilisation de l'IA par les forces de l'ordre](#)
- [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](#)
- [Rapport 4 : L'IA durant le procès et en appel](#)
- [Rapport 5 : L'IA et les mécanismes de surveillance systémiques](#)

Ensemble, les rapports présentaient une analyse « du cycle de vie » de l'IA dans tout le système canadien de justice pénale.

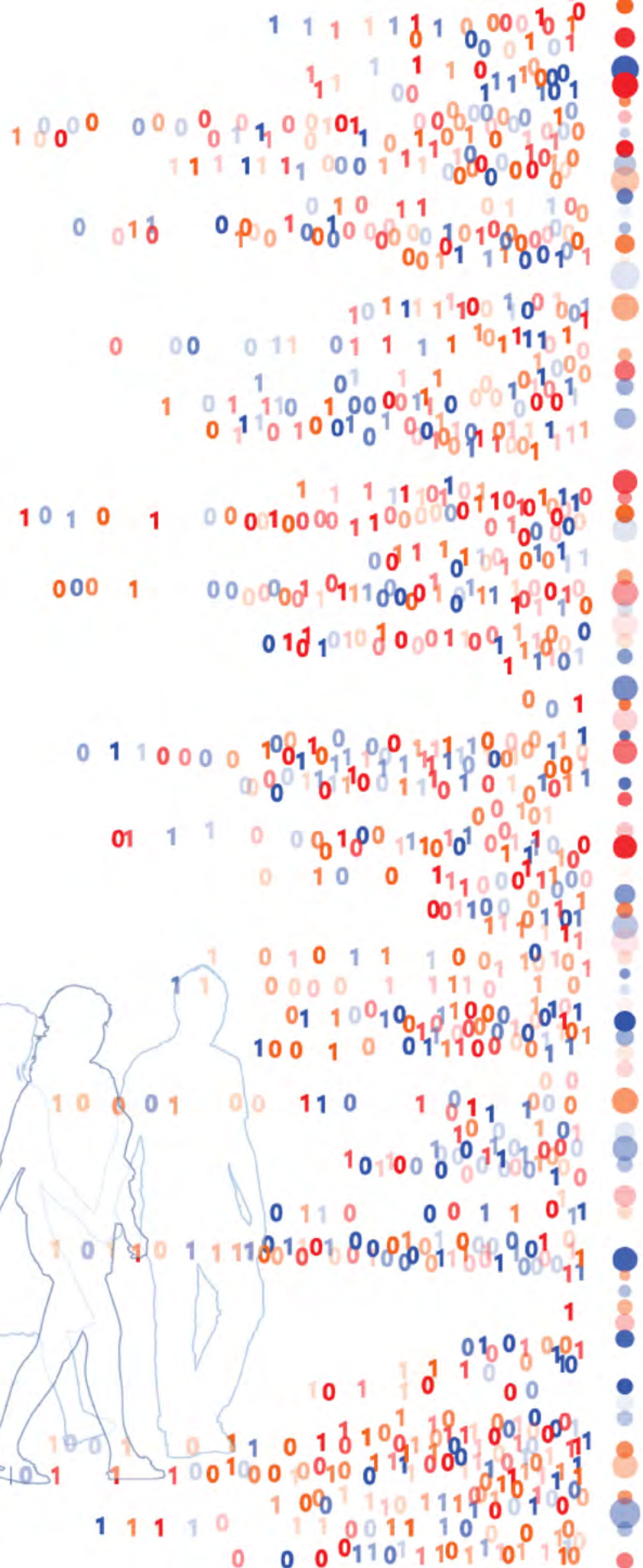
Outre les documents thématiques du projet, la CDO a organisé deux tables rondes d'une demi-journée afin d'examiner les principaux enjeux liés à l'IA dans le domaine de la justice pénale, y compris une [table ronde sur l'utilisation de la technologie de reconnaissance faciale par les forces de l'ordre à Vancouver](#) en juin 2025 et une [table ronde sur l'IA comme preuve en justice pénale à Toronto](#) en août 2025.

Les [membres du groupe consultatif du projet](#) et les [auteurs des rapports](#) comprennent des représentants des gouvernements, des services policiers, des avocats de la Couronne, des avocats de la défense, des services d'aide juridique, des services administratifs des tribunaux, des commissions des droits de la personne et de la protection de la vie privée, d'organisations civiles et d'intérêt public, ainsi que du milieu universitaire.

Ce projet a donné lieu à de nombreuses consultations et à une large mobilisation au sein du système de justice pénale provincial et canadien. Au total, plus de 1 400 personnes ont participé à plus de 30 débats, ateliers et conférences publics partout au Canada.

La CDO a également bénéficié d'un partenariat solide en matière de recherche et de consultation avec l'[Initiative d'IA et de justice pénale UBC](#), dirigée par le professeur Benjamin Perrin, de la Faculté de droit Peter A. Allard de l'Université de la Colombie-Britannique.

Tous les documents du projet de la CDO concernant l'IA dans le système de justice pénale sont accessibles sur la [page Web de la CDO](#).





Introduction

Voici le sommaire du Rapport final et des recommandations de la Commission du droit de l'Ontario (CDO) concernant le [projet sur l'intelligence artificielle dans le système de justice pénale](#) (« projet sur l'IA dans le système de justice pénale »).

L'IA est de plus en plus utilisée dans les systèmes de justice pénale au Canada et dans le monde entier pour faciliter les enquêtes, analyser les éléments de preuve, évaluer les risques, préparer les observations et les jugements, et mieux utiliser les ressources. Parmi les outils d'IA figurent la surveillance biométrique et la technologie de reconnaissance faciale (RF), le maintien de l'ordre prédictif, les lecteurs automatiques de plaques d'immatriculation (LAPI), la surveillance des réseaux sociaux, l'analyse de documents et de vidéos, les algorithmes de mise en liberté sous caution et de détermination de la peine, les drones, la rédaction de rapports par IA, et bien d'autres encore.

De nombreuses technologies d'IA peuvent contribuer à renforcer la sécurité publique, à améliorer les enquêtes policières ainsi qu'à accroître l'efficacité et l'équité des procédures pénales. Cependant, les systèmes d'IA dans le secteur pénal, tels que le maintien de l'ordre prédictif, la RF et les systèmes d'IA générative, présentent des risques avérés pour les droits de la personne, la procédure pénale, la vie privée et l'accès à la justice. Ces risques touchent plus particulièrement les communautés racisées et à faible revenu.

Dans de nombreux pays, les systèmes d'IA dans le secteur pénal sont très répandus, en pleine expansion et font l'objet de controverses. En Angleterre et au Pays de Galles, par exemple, plus de 4,6 millions de visages ont été analysés par des systèmes de reconnaissance faciale en temps réel en 2024¹. Les outils d'IA dans le secteur pénal sont également largement utilisés aux États-Unis, y compris un réseau comptant quelque 140 000 LAPI².

Dans ces exemples parmi d'autres, les systèmes d'IA dans le secteur pénal sont tantôt salués pour leur contribution à l'amélioration de la sécurité publique, tantôt critiqués pour la surveillance de masse qu'ils permettent, leurs biais, leurs violations des droits procéduraux, ainsi que leurs erreurs et leurs hallucinations. En réponse, de nombreux gouvernements et autres institutions ont adopté des lois et des politiques en faveur d'une « IA responsable » afin de promouvoir les avantages des systèmes d'IA dans le secteur pénal tout en contrôlant leurs limites et leurs risques prévisibles.

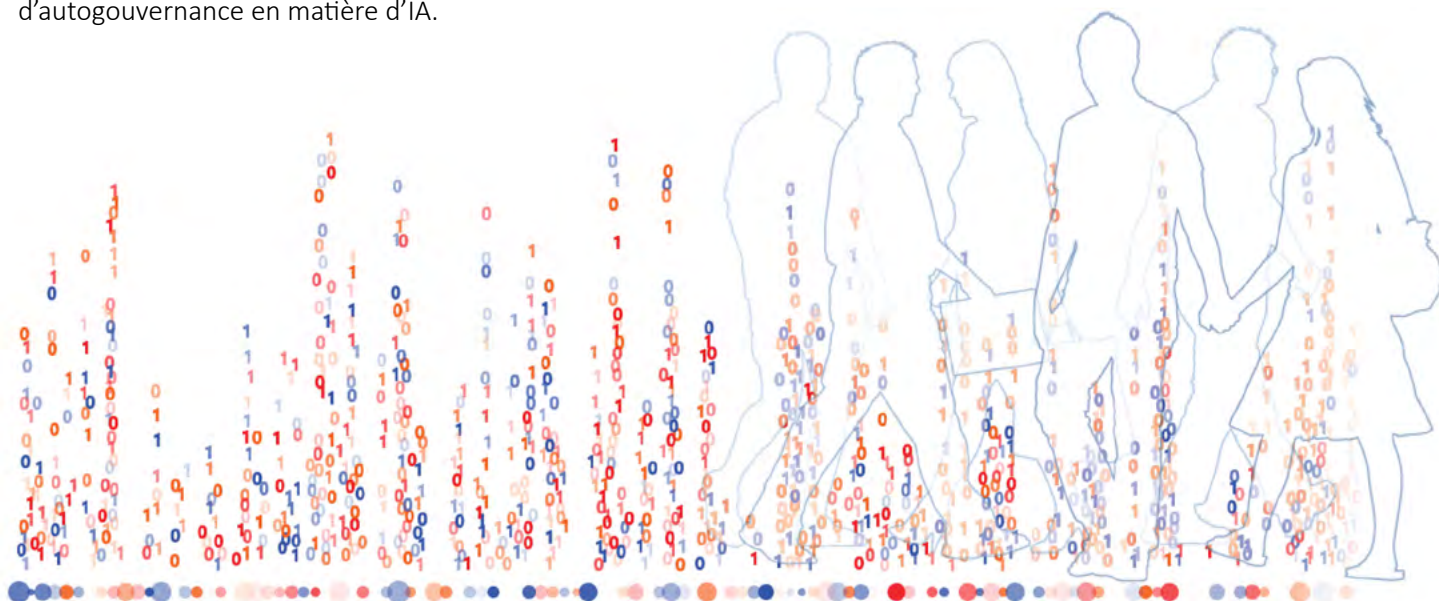
Par rapport à de nombreux autres pays, le Canada a été plus lent à déployer l'IA dans son système pénal. Des rapports indiquent toutefois que de nombreux services de police canadiens ont testé ou mis en œuvre toute une gamme de systèmes d'IA, notamment la RF, les LAPI, la reconnaissance d'objets, le maintien de l'ordre prédictif et les drones. Au Canada, des procureurs, des avocats de la défense et des tribunaux commencent également à utiliser des systèmes d'IA.

L'adoption d'une gouvernance responsable de l'IA dans le secteur pénal au Canada semble également plus lente. À ce jour, aucun gouvernement canadien n'a adopté de lois ou de règlements régissant l'utilisation de l'IA par les forces de l'ordre ou les tribunaux pénaux canadiens. Cela dit, de nombreux services policiers canadiens et d'autres institutions du système de justice pénale ont élaboré des politiques d'autogouvernance en matière d'IA.

La CDO estime que les systèmes d'IA utilisés dans le secteur pénal introduisent des risques nouveaux et complexes susceptibles d'exposer un nombre sans précédent d'Ontariens et d'Ontariennes à la surveillance policière, à des atteintes à la vie privée, à des biais raciaux ainsi qu'à d'autres risques et préjudices.

La CDO et de nombreuses parties prenantes craignent que la combinaison de multiples lois, d'institutions diverses et de technologies complexes n'entraîne une gouvernance ponctuelle, incohérente ou inappropriée des systèmes d'IA utilisés à des fins pénales. La CDO et d'autres estiment que la réponse provinciale à ces risques doit être coordonnée et systémique afin de garantir que ces systèmes soient légaux, bénéfiques et inspirent confiance au public.

Les 29 recommandations de la CDO visent à intégrer des principes et des politiques relatifs à une IA responsable dans l'ensemble du système de justice de l'Ontario. L'une des principales conclusions de ce projet est la volonté quasi unanime des parties prenantes de la justice pénale de collaborer afin d'aborder de manière constructive les enjeux liés à l'IA dans le secteur pénal. Le texte intégral du rapport final et des recommandations du projet de la CDO sur l'IA dans le système de justice pénale est disponible [ici](#).



L'IA dans le secteur pénal au Canada

On ignore dans quelle mesure l'IA est utilisée par la police et d'autres institutions de la justice pénale au Canada. Le rapport de l'UBC sur l'utilisation de l'IA par la police, les renseignements divulgués par les services policiers et les articles parus dans la presse laissent entendre que les services policiers canadiens figurant ci-dessous ont utilisé ou utilisent actuellement les systèmes d'IA suivants³ :

Technologie de reconnaissance faciale

- Service de police de Calgary
- Service de police d'Edmonton
- Service de police de la région de Halton
- Service de police d'Ottawa
- Service de police de la région de Peel
- GRC
- Service de police de Thunder Bay
- Service de police de Toronto
- Service de police de la région de York

Lecteurs automatiques de plaques d'immatriculation

- Service de police d'Ottawa
- GRC
- Service de police de Toronto
- Service de police de Victoria

Reconnaissance d'objets et analyse vidéo

- GRC
- Service de police de Thunder Bay
- Service de police de Toronto
- Service de police de Winnipeg

Maintien de l'ordre prédictif

- Service de police de Calgary
- Service de police de Vancouver
- Service de police de Saskatoon

Robots, drones et véhicules autonomes

- Jusqu'à 17 services de police en Ontario
- GRC
- Service de police de Vancouver
- Service de police de Winnipeg

Détection de coups de feu

- Service de police de Toronto

Collecte de renseignements de sources ouvertes et surveillance des médias sociaux

- Service de police de Calgary
- GRC

Rapports de police assistés par l'IA

- Service de police de Fredericton
- Service de police d'Ottawa
- Service de police de Peel



Les systèmes d'IA dans le secteur pénal et leur potentiel

La section 2 du rapport final passe en revue les systèmes d'IA les plus couramment utilisés dans le secteur de la justice pénale aux États-Unis, au Royaume-Uni et au Canada. La plupart sont des systèmes policiers ; toutefois, l'IA est également utilisée par les procureurs, les tribunaux et d'autres parties⁴.

Les recherches et les consultations de la CDO démontrent que, selon la manière dont ils sont déployés, les systèmes d'IA présentent un potentiel considérable pour améliorer la sécurité publique et le système de justice pénale. Les systèmes d'IA utilisés par les services policiers servent notamment, et le plus souvent, à :

- Identifier des personnes inconnues ou vérifier leur identité.
- Suivre les déplacements et la localisation des personnes.
- Gérer et analyser de grands ensembles de données ou de documents.
- Analyser des éléments de preuve.
- Prédire les lieux où des crimes pourraient être commis ou identifier leurs auteurs potentiels.
- Rédiger des rapports de police, transcrire ou traduire des enregistrements.

Parmi les systèmes d'IA utilisés par les services policiers les plus connus ou les plus courants, on peut citer les trois suivants :

Technologie de reconnaissance faciale (RF)

La technologie de RF compare une « empreinte faciale » à une image de référence stockée dans une base de données et détermine si les images correspondent. Il existe de nombreux types et variantes de RF, notamment des systèmes utilisés pour identifier des suspects, dans les enquêtes sur les personnes disparues ou sur la traite des personnes, dans les enquêtes sur l'exploitation sexuelle d'enfants, ainsi que pour la surveillance des foules et la vérification de l'identité.

Il existe des différences juridiques et opérationnelles importantes entre les différents systèmes de RF. Par exemple, la RF en temps réel analyse les images provenant de flux vidéo en direct afin d'identifier ou de suivre des personnes en temps réel. À l'inverse, la RF à posteriori, sert à identifier des personnes à partir d'images ou de vidéos enregistrées dans le passé.

C'est sans doute au Royaume-Uni que le déploiement de la RF en temps réel est le plus étendu, où un système national à grande échelle est actuellement mis en place. Le Royaume-Uni utilise des véhicules mobiles équipés de technologie de RF en temps réel et des caméras fixes pour analyser les foules et comparer les visages à une liste de surveillance de la police en temps réel⁵. La RF serait utilisée par près de 1 000 organismes chargés de l'application de la loi aux États-Unis⁶.

On ignore combien de services policiers au Canada utilisent la RF, en raison de l'absence d'obligation de divulgation des systèmes d'IA utilisés par les forces de l'ordre. Le rapport de l'UBC sur l'utilisation de l'IA par la police indique que la RF a été utilisée par au moins cinq services policiers de l'Ontario, notamment ceux de Thunder Bay, de la région de York, de la région de Peel, de la région de Halton et de Toronto⁷.

L'utilisation des systèmes de RF par les services policiers canadiens est en pleine expansion. Par exemple, les services de police d'Ottawa et d'Edmonton ont récemment annoncé la mise en place de nouveaux systèmes de RF ou les ont déjà rendus opérationnels. Le système d'Edmonton mérite une mention particulière : la police d'Edmonton a commencé à tester des caméras corporelles équipées d'un système de RF entraîné à détecter les visages d'environ 7 000 personnes figurant sur une liste de surveillance, à partir de photos d'identité judiciaire de personnes qui, selon la police, font l'objet de mandats d'arrêt pour des infractions graves ou qui sont signalées comme représentant un risque pour la sécurité.

Lecteurs automatiques de plaques d'immatriculation (LAPI)

Les LAPI et les systèmes de surveillance de véhicules utilisent des caméras mobiles ou fixes pour détecter des renseignements, comme le numéro de plaque d'immatriculation et autres. Les LAPI ont été décrits comme des « empreintes de véhicules ». Ils aident la police à retrouver rapidement les véhicules volés ainsi que les conducteurs sans permis, sans assurance, ou dont le permis est suspendu. Les LAPI peuvent également être utilisés pour repérer des individus.

L'ampleur de la surveillance par LAPI est sans précédent : en 2025, le Service de police de Los Angeles a balayé plus de 210 millions de plaques d'immatriculation en deux mois⁸.

On ignore dans quelle mesure les LAPI sont déployés en Ontario ou au Canada. Le Service de police de Toronto indique qu'il utilise ces systèmes pour recevoir des alertes en temps réel dans les véhicules de patrouille afin d'arrêter des criminels recherchés, de retrouver des véhicules volés et de localiser des personnes disparues figurant sur diverses listes. Le Service de police de Toronto précise que ses LAPI peuvent balayer plus de 1,25 million de plaques d'immatriculation chaque jour⁹.



Maintien de l'ordre prédictif

Le maintien de l'ordre prédictif est un terme générique désignant des systèmes d'IA qui traitent et analysent des ensembles de données volumineux et complexes beaucoup plus rapidement que les humains. Le maintien de l'ordre prédictif recouvre de nombreuses applications, mais il est généralement défini comme l'ensemble des systèmes d'IA qui tentent de prédire la criminalité, notamment : 1) les systèmes géolocalisés, qui prédisent où et quand des activités criminelles pourraient se produire et 2) les systèmes personnels, qui prédisent qui est susceptible d'être impliqué dans des activités criminelles futures.

Le maintien de l'ordre prédictif est largement utilisé aux États-Unis. Parmi les services policiers canadiens qui utilisent ou testent cette approche, on peut citer ceux de Vancouver (GeoDASH) et de Calgary (Palantir Gotham).

Autres systèmes d'IA utilisés par les forces de l'ordre

Parmi les autres systèmes d'IA utilisés ou envisagés par les forces de l'ordre, on peut citer les systèmes de renseignements d'origine source ouverte et de renseignements issus des réseaux sociaux; les drones; les rapports de police assistés par l'IA; la gestion de la preuve; la détection de coup de feu; les algorithmes de mise en liberté sous caution et de détermination de la peine, ainsi que l'inférence biométrique.

Tribunaux pénaux, procureurs et avocats de la défense

Les services policiers ne sont pas les seules institutions du système de justice pénale à utiliser l'IA. Les procureurs peuvent recourir à l'IA pour faciliter la gestion de la preuve numérique, automatiser les expurgations, rationaliser la production de documents et analyser la preuve médico-légale. Les tribunaux ont utilisé l'IA pour faciliter la rédaction des jugements; la recherche juridique, la rédaction et la traduction; pour générer des transcriptions et pour aider les justiciables à remplir et à déposer des formulaires. Les avocats et les justiciables non représentés peuvent utiliser des systèmes d'IA pour effectuer des recherches juridiques et rédiger des textes, des mémoires et des observations; pour évaluer des éléments de preuve; pour vérifier des témoignages ou pour résumer des transcriptions, analyser des rapports d'experts et préparer des contreinterrogatoires.





Préjudices et risques liés à l'IA en droit pénal

La section 3 du rapport final aborde les risques et les préjudices potentiels liés à l'IA dans le système de justice pénale¹⁰.

Risques juridiques

Biais et discrimination

Il a été démontré que de nombreux systèmes de RF sont biaisés et discriminatoires. Plusieurs opposants estiment que ces biais sont une preuve irréfutable pour interdire complètement ou partiellement ces systèmes. D'autres croient que l'importance de ce biais diminue et qu'une amélioration des données d'entraînement ou des systèmes peut atténuer les erreurs.

De nombreux systèmes de maintien de l'ordre prédictif se sont également révélés biaisés et discriminatoires, ce qui a conduit au retrait de bon nombre d'entre eux face aux contestations judiciaires et au tollé général. D'autres systèmes d'IA dans le secteur pénal ont suscité d'importantes inquiétudes quant à leur biais, en particulier les algorithmes de mise en liberté sous caution et de détermination de la peine.

Vie privée et surveillance

Les risques liés à la protection de la vie privée et à la surveillance sont parmi les plus largement débattus en ce qui concerne les systèmes d'IA dans le secteur pénal, en particulier les systèmes de RF. Ces risques dépendent grandement de l'utilisation qui est faite de ces systèmes. Par exemple, un système de RF en direct surveillant une manifestation publique comporte des risques plus graves pour les droits constitutionnels et la vie privée qu'un système de RF à posteriori qui compare un suspect à une base de données d'enquête ou de photos d'identité judiciaire.

L'exemple du déploiement de la RF au Royaume-Uni illustre les risques liés à la protection de la vie privée de cette technologie lorsqu'elle est déployée à grande échelle. Au Royaume-Uni, les services policiers ont utilisé des fourgons équipés de la RF en temps réel et des caméras fixes de RF en direct pour surveiller des millions de personnes, dont plus de 3 millions à Londres en une seule année¹¹. Au Royaume-Uni, la RF en temps réel permet de surveiller les personnes dans les « zones sensibles », dans les principaux quartiers commerçants, dans les trains et le métro, lors d'événements sportifs et de festivals de musique, ainsi que dans d'autres lieux.

Les systèmes de RF utilisés par les services policiers canadiens ont également fait l'objet de critiques pour des raisons liées à la vie privée et à la surveillance, notamment en raison de l'utilisation de ClearviewAI par la GRC et du projet pilote de reconnaissance faciale par caméra corporelle mené par le Service de police d'Edmonton.

Les LAPI ont été vivement critiqués pour leurs atteintes à la vie privée et pour favoriser la surveillance de masse. L'utilisation de drones par les forces de l'ordre soulève également d'importantes questions en matière de vie privée et de surveillance, tout comme les systèmes d'IA dans le secteur pénal, tels que l'analyse vidéo, la surveillance des médias sociaux et le maintien de l'ordre prédictif.

Communication d'informations et transparence

La communication d'informations et la transparence sont des éléments fondamentaux de la responsabilité juridique et publique, en particulier dans le cadre des poursuites pénales. Les systèmes d'IA dans le secteur pénal ont été critiqués pour 1) leur manque de transparence ou de divulgation publique concernant l'existence d'un tel système et 2) l'absence de communication d'informations à une personne accusée au cours d'une enquête ou d'une procédure pénale.

Au Canada, il n'existe pas d'obligation de divulgation exhaustive des systèmes d'IA utilisés par la police ou par d'autres instances du secteur de justice pénale. La GRC et le Service de police de Toronto ont mis en place des politiques internes exigeant la divulgation de leurs systèmes d'IA. Ces politiques ne sont toutefois pas harmonisées.

L'explicabilité et le problème des « boîtes noires »

Les systèmes d'IA 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 prises à l'aide de l'IA « encore plus impénétrables que les jugements humains »¹². De ce fait, même les systèmes algorithmiques et d'IA les plus simples peuvent devenir des « boîtes noires » complexes et opaques. Cette opacité et ce manque d'explicabilité constituent un problème particulier dans le domaine de la justice pénale.

Exactitude, fiabilité et validité des données

L'exactitude, la fiabilité et la validité des données sont essentielles au succès et à la légitimité des systèmes d'IA utilisés par les services policiers, les pouvoirs publics ou les tribunaux. Les données d'entraînement des systèmes de RF et de maintien de l'ordre prédictif en particulier ont fait l'objet de vives critiques. L'exactitude, la fiabilité et la validité des systèmes de RF peuvent également varier en fonction de la manière dont ils sont utilisés et du moment où ils le sont. INTERPOL note, par exemple, que « ... l'exactitude des [systèmes de reconnaissance faciale]... varie considérablement en fonction de la qualité de l'image fournie au système »¹³.

Après avoir examiné les données issues des tests d'IA menés par la police, le projet « Initiative d'IA et de justice pénale » de l'Université de la Colombie-Britannique (UBC) a conclu ceci :

Il existe très peu de preuves scientifiques indépendantes démontrant que de nombreuses technologies d'IA policière sont précises, fiables, efficaces ou nécessaires. Malgré des affirmations généralisées en matière d'efficacité et d'objectivité, des préoccupations significatives subsistent concernant les taux d'erreur documentés, l'amplification des biais et les faux positifs¹⁴.

Risques liés à la gouvernance

Outre les risques juridiques, les recherches et les consultations de la CDO ont révélé que les systèmes d'IA utilisés dans le système de justice pénale présentent d'importants risques en matière de gouvernance en Ontario.

Les risques liés à une gouvernance décentralisée et fragmentée de l'IA dans le secteur pénal découlent de deux raisons :

D'abord, il existe de nombreuses lois et instances de réglementation qui régissent les systèmes d'IA dans le secteur pénal en Ontario, notamment :

- La *Charte des droits et libertés*.
- Le *Code criminel* du Canada.
- Les lois sur les droits de la personne et la protection des renseignements personnels.
- Le droit de la preuve, les règles de procédure, les principes de la common law et les textes législatifs connexes.
- Les règlements, les directives ou les politiques du fédéral et des provinces en matière de police.
- Les politiques ou les directives émanant des commissions de police, des services policiers et des organismes provinciaux.
- Les décisions et les directives émanant des tribunaux, des commissions chargées de la protection de la vie privée et des droits de la personne, des barreaux et d'autres organismes.

Ensuite, il existe en Ontario un réseau provincial vaste, diversifié et décentralisé d'institutions qui pourraient être impliquées dans l'exploitation, la supervision, les litiges ou le jugement des allégations criminelles liées à l'IA dans le secteur pénal, notamment :

- Les 53 services policiers de l'Ontario.
- Les commissions de service de police, les municipalités et les administrations régionales.
- Les ministères provinciaux du Solliciteur général et du Procureur général.
- L'inspecteur général des services policiers et l'Agence des plaintes contre les forces de l'ordre.
- Les procureurs de la Couronne.
- Les juges de droit pénal siégeant à la Cour de justice de l'Ontario et à la Cour supérieure.
- Les avocats de la défense au criminel, les avocats de service et Aide juridique Ontario.
- Les juges de paix.

La combinaison de multiples lois, d'acteurs et d'institutions variés, ainsi que de technologies complexes, pourrait entraîner une gouvernance ponctuelle, incohérente ou inadéquate des systèmes de RF à des fins pénales, en particulier si ces systèmes venaient à être déployés à grande échelle dans tout l'Ontario.

De plus, la CDO a été fréquemment informée des risques et des défis liés au déploiement ou à l'exploitation de l'IA au sein des institutions de la justice pénale. Par exemple, les services policiers ont souvent décrit les efforts considérables nécessaires pour intégrer des pratiques responsables en matière d'IA au sein de leurs organisations, notamment, les politiques internes et les ressources consacrées à la conformité juridique, à l'approvisionnement, aux évaluations de l'IA, à la formation, à la supervision humaine, à la gestion des données, à la gestion de la preuve, à l'évaluation de la souveraineté numérique, etc. Il s'agit là de tâches complexes et couteuses, potentiellement hors de portée de toutes les institutions de la justice pénale, à l'exception des plus grandes et des mieux dotées en ressources.

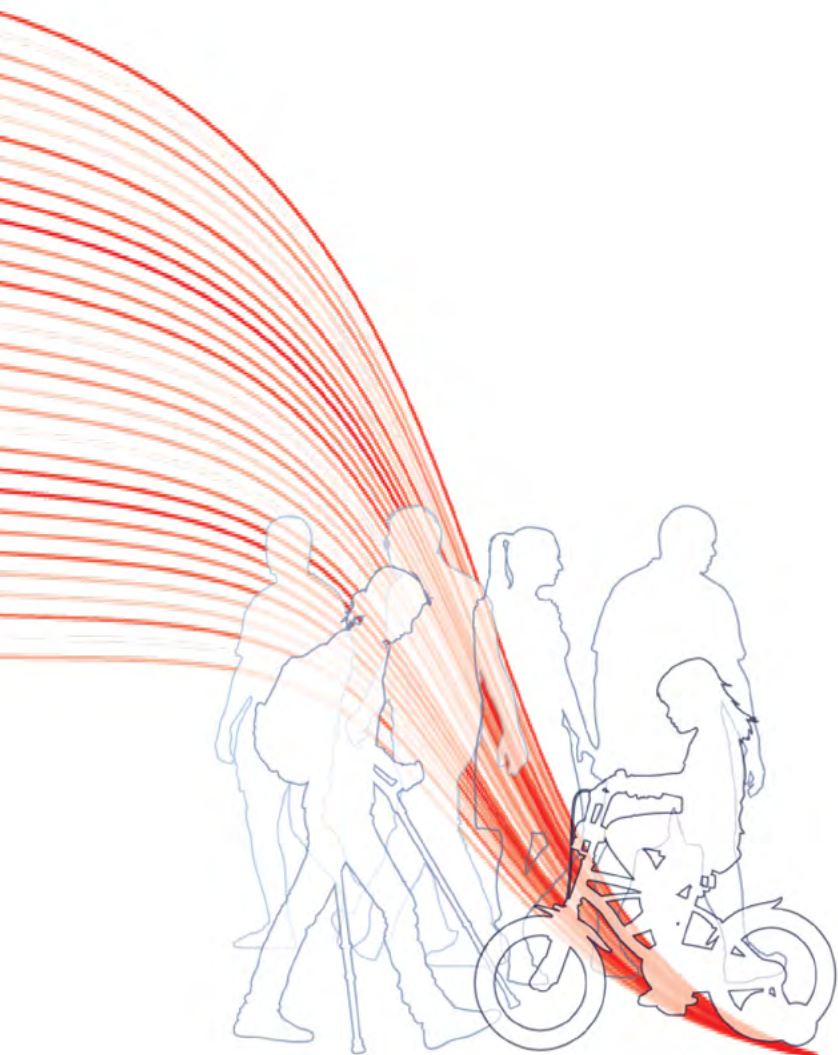
Nos consultations et nos recherches ont mis en évidence des efforts complexes, déployés au sein et entre de nombreux services policiers canadiens pour traiter de manière proactive les enjeux institutionnels, notamment des initiatives remarquables menées par la GRC, le Service de police de Toronto et l'Association canadienne des chefs de police (ACCP). Cette approche, bien que louable, comporte des risques et des lacunes. Par exemple, de nombreux services ont évoqué la nécessité d'élaborer des politiques communes ou cohérentes en matière d'étude d'impact sur l'IA dans le domaine pénal, de conformité ou d'approvisionnement. De nombreuses personnes consultées ont également indiqué que les institutions tentaient de résoudre le même problème en même temps.

Risques liés à l'administration de la justice et à l'accès à la justice

Les risques décrits ci-dessus soulèvent de nouveaux défis complexes en matière d'administration de la justice et d'accès à la justice. Par exemple, il n'est pas certain que les tribunaux disposent des capacités ou des outils nécessaires pour traiter les questions complexes et systémiques d'ordre statistique, technique, politique et juridique qui se poseront dans les affaires pénales impliquant des preuves issues de l'IA.

De même, il sera très difficile pour la plupart des personnes accusées d'infractions criminelles (en particulier celles qui sont représentées par l'aide juridique ou qui se représentent elles-mêmes) de contester efficacement les questions statistiques, techniques et juridiques complexes soulevées par les systèmes d'IA, notamment lors des audiences relatives à la mise en liberté sous caution ou à la détermination de la peine.

Les implications juridiques et sociales liées aux risques en matière d'administration de la justice et d'accès à la justice sont préoccupantes. Il est possible que seuls les justiciables les mieux pourvus soient en mesure de contester les systèmes d'IA dans le secteur pénal. En conséquence, ces systèmes pourraient créer de nouveaux obstacles importants pour les communautés à faible revenu, marginalisées, autochtones et racisées, aggravant ainsi la surreprésentation de ces communautés au sein du système judiciaire de l'Ontario.





IA responsable dans le secteur pénal

La section 4 du rapport final passe en revue les questions relatives à l'IA responsable dans le système de justice pénale à l'échelle internationale et au Canada¹⁵.

À l'échelle internationale

Les avantages, risques et inconvénients potentiels de l'IA dans le système de justice pénale sont largement documentés et reconnus par les gouvernements, les services policiers, les procureurs, les avocats de la défense, les universitaires et les ONG du monde entier.

Cette reconnaissance a donné lieu à un ensemble diversifié de lois, de politiques, de cadres réglementaires et d'initiatives connexes « dignes de confiance » ou « responsables » en matière d'IA dans le secteur pénal. Ces initiatives partent du principe que les avantages de l'IA dépendent de règles spécifiques et complexes pour atténuer les risques et les préjudices.

Le fond et la forme de ces initiatives varient considérablement. Leur fil conducteur demeure toutefois la nécessité d'établir une gouvernance cohérente et globale de l'IA dans le secteur pénal, qui pourrait couvrir les points suivants :

- Communication obligatoire des systèmes d'IA dans le secteur pénal, y compris la mise en place de « registres publics d'IA ».
- Interdiction des systèmes d'IA dans le secteur pénal présentant le plus haut niveau de risque.
- Critères permettant d'identifier les systèmes interdits, à haut risque et à usage restreint.
- Limitations de la finalité et de l'utilisation.
- Études d'impact et évaluations des risques obligatoires et transparentes de l'IA.
- Exigences en matière d'atténuation des risques.
- Obligations de mesurer, de corriger et de contrôler les biais.
- Garanties procédurales et probatoires.
- Exigences obligatoires en matière d'intervention humaine et d'apprentissage.
- Exigences obligatoires en matière d'audit et d'évaluation.

- Procédures d'évaluation définies pour les projets pilotes et les « bacs à sable ».
- Surveillance indépendante des systèmes individuels et des systèmes d'IA dans le secteur pénal.

Le règlement sur l'intelligence artificielle de l'Union européenne

Le cadre international le plus important en matière de gouvernance de l'IA est le règlement sur l'intelligence artificielle de l'Union européenne (règlement de l'UE sur l'IA)¹⁶. Le règlement de l'UE sur l'IA est une législation-cadre de grande envergure qui régit le développement et l'utilisation des systèmes d'IA dans toute l'Union européenne, y compris les systèmes utilisés tant dans le secteur privé que public. À ce jour, le règlement de l'UE sur l'IA constitue sans doute le régime législatif le plus complexe au monde en matière de responsabilité liée à l'IA dans le secteur pénal.

L'article 5 du chapitre II du règlement de l'UE sur l'IA énonce plusieurs « risques inacceptables » et interdictions concernant certains systèmes d'IA, notamment une interdiction partielle de la RF en temps réel à grande échelle et de la surveillance biométrique¹⁷ ainsi qu'une interdiction partielle du maintien de l'ordre prédictif¹⁸. L'article III du règlement de l'UE sur l'IA définit également de manière préventive plusieurs systèmes d'IA dans le secteur pénal comme « à haut risque », notamment les algorithmes de mise en liberté sous caution et de détermination de la peine, ainsi que les éléments de preuve générés par l'IA dans les procès pénaux¹⁹. Dans le cas où la police ou les pouvoirs publics déploieraient ces systèmes, le règlement de l'UE sur l'IA impose de nombreuses exigences en matière de contrôle et d'atténuation des risques.

États-Unis

Le gouvernement fédéral américain a connu des changements radicaux en matière de règles et de politiques relatives à l'utilisation responsable de l'IA dans le secteur pénal. L'administration Biden a mis en place un cadre complet régissant l'utilisation responsable de l'IA dans le secteur pénal, avec des exigences détaillées concernant jusqu'à 18 systèmes d'IA ayant une « incidence sur les droits » utilisés par les départements et agences américains dans le secteur de la justice pénale²⁰. En janvier 2025, ces exigences ont été abrogées par l'administration Trump.

Aux États-Unis, il est courant que les autorités étatiques et locales réglementent l'utilisation de la RF ; en août 2026, on comptait plus de 30 lois étatiques ou municipales interdisant ou limitant cette utilisation²¹. Ces lois comprennent :

- les interdictions catégoriques ;
- les exigences relatives au mandat, à la cause probable ou à l'ordonnance judiciaire ;
- les prescriptions liées aux crimes graves ;
- les interdictions d'utiliser la RF avec les caméras corporelles ;
- l'obligation d'informer les accusés du fait que les forces de l'ordre utilisent la RF ;
- les obligations de déclaration ;
- les règles excluant un seul fondement, c'est-à-dire que la RF ne peut pas constituer le seul motif d'une arrestation.

La réglementation sur les drones est également courante : pas moins de 18 États américains ont adopté des lois obligeant les services policiers à obtenir un mandat de perquisition pour utiliser des drones à des fins de surveillance ou pour mener une perquisition²².

Une polémique nationale agite actuellement les États-Unis au sujet des LAPI : la contestation contre les caméras « Flock » (du nom de Flock Safety, l'un des principaux fournisseurs américains de LAPI) a été rapide, bipartisane et décisive. Les LAPI ont été vivement critiqués pour leurs atteintes à la vie privée, pour leur rôle dans la surveillance de masse, pour leur inefficacité, pour leur contribution au racisme systémique dans les pratiques policières et pour le partage non autorisé de données avec des autorités fédérales, notamment les services d'immigration.

DeFlock, un organisme de pression américain, indique que 153 villes ont annulé ou rejeté des contrats de LAPI ou désactivé des caméras depuis 2021, dont plus de 50 rien qu'au mois d'août 2026²³. Le gouverneur républicain de Floride a récemment déclaré que l'utilisation des LAPI en Floride était « hors de contrôle »²⁴ et a ordonné le retrait des caméras de LAPI des routes de l'État, déclarant (traduction libre) : « Ce que nous ne voulons pas en Floride, c'est un État de surveillance numérique basé sur l'IA où tout ce que nous faisons est surveillé en permanence²⁵. »

Royaume-Uni

Le développement de la RF au Royaume-Uni a été rapide et controversé, ce système ayant été décrit comme « hors de contrôle »²⁶. De nombreux détracteurs, dont le commissaire à l'égalité et aux droits de la personne du Royaume-Uni, ont souligné les risques de violations de la vie privée, de préjugés raciaux et de harcèlement policier. Les détracteurs affirment également que le déploiement rapide de la RF se poursuit faute de cadre législatif et politique.

En mai 2026, le gouvernement britannique a annoncé son intention de mettre en place un nouveau cadre juridique afin d'étayer l'utilisation, par les forces de l'ordre, de la reconnaissance faciale et de technologies similaires²⁷. En juin 2026, le gouvernement britannique a annoncé la création de PoliceAI, « un nouveau centre national dédié au développement, à l'expérimentation et au déploiement responsables de l'intelligence artificielle dans le domaine policier »²⁸.

Canada

Contrairement à l'Union européenne, aux États-Unis et au Royaume-Uni, il n'existe au Canada aucune loi, aucun règlement ni politique fédérale ou provinciale spécifique régissant les systèmes d'IA dans le secteur pénal.

Gouvernement fédéral

Il n'existe aucune législation fédérale régissant les systèmes d'IA dans le secteur pénal au Canada. La *Loi sur l'intelligence artificielle et les données (LIAD)*, projet de loi fédéral qui n'a pas abouti, aurait intégré plusieurs principes d'IA responsable et établi un cadre de gouvernance limité, fondé sur les risques, pour les systèmes d'IA du secteur privé au Canada²⁹, mais n'aurait pas réglementé directement l'utilisation de l'IA dans le secteur public ni dans le système de justice pénale. Il n'y a pas non plus eu de modifications spécifiques à l'IA apportées au *Code criminel* du Canada ou à d'autres lois fédérales pertinentes.

En mai 2026, le gouvernement fédéral a présenté la *Stratégie nationale en matière d'intelligence artificielle du Canada : L'IA pour tous*³⁰. Toutefois, la Stratégie n'a pas établi de cadre pour une IA digne de confiance dans le système de justice pénale. Elle ne semble pas non plus promouvoir une IA responsable par la réglementation des entreprises du secteur privé fournissant des systèmes d'IA dans le secteur pénal, comme la *LIAD* aurait pu le faire.

Depuis l'annonce de la *Stratégie*, le gouvernement fédéral a présenté deux nouveaux projets de loi relatifs à l'IA : le projet de loi C-34 (*Loi sur les médias sociaux sécuritaires*)³¹ et le projet de loi C-36 (*Loi visant à protéger la vie privée et les données des consommateurs*), qui actualise la législation en matière de protection des renseignements personnels dans le secteur privé³². Aucun de ces deux projets de loi ne traite de l'IA responsable dans le secteur pénal.

La principale initiative fédérale en matière d'IA responsable est la *Directive sur la prise de décisions automatisée* (Directive fédérale sur la PDA) et l'Outil d'évaluation de l'incidence algorithmique (EIA)³³. La Directive fédérale sur la PDA et l'EIA ne s'appliquent pas explicitement aux services fédéraux chargés de l'application de la loi; toutefois, la GRC s'y est conformée de son plein gré, en publiant 14 rapports sur le Registre de l'IA du gouvernement du Canada³⁴.

Gouvernement de l'Ontario

Le gouvernement de l'Ontario a pris des mesures importantes pour mettre en place une gouvernance responsable de l'IA dans le secteur public ontarien, mais ces initiatives ne concernent pas le secteur de la justice pénale provincial. Par conséquent, il n'existe pas de cadre de gouvernance responsable de l'IA dans le secteur pénal en Ontario.

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 2024³⁵. La LRSCN a pour objectif de définir l'intelligence artificielle (IA) afin d'assurer la cohérence au sein du secteur public et de mettre en place des mesures de protection visant à garantir une utilisation responsable des systèmes d'IA³⁶. La LRSCN confère le pouvoir de prescrire, par voie réglementaire, un large éventail d'actes de gouvernance de l'IA, notamment des interdictions relatives à l'IA, des mesures de gestion des risques, des obligations de divulgation publique, des normes techniques et la désignation de personnes chargées de la surveillance³⁷. La LRSCN ne s'applique pas à l'IA utilisée dans le système de justice pénale de l'Ontario.

Le gouvernement provincial a donné suite à la LRSCN en adoptant, en décembre 2024, sa « Directive sur l'utilisation responsable de l'intelligence artificielle », mais celle-ci ne s'applique pas explicitement aux systèmes d'IA utilisés par la police ontarienne ou dans les tribunaux pénaux de l'Ontario³⁸.

Services policiers canadiens

Contrairement aux gouvernements fédéral et provinciaux, plusieurs services policiers canadiens ont pris des mesures importantes pour mettre en place des cadres complets et responsables en matière d'IA dans le secteur pénal.

Au niveau fédéral, le Programme national d'intégration des technologies (PNIT) et le Plan de transparence de la GRC sont des initiatives complexes qui intègrent de nombreux principes relatifs à l'utilisation responsable de l'IA dans le secteur pénal.

De nombreux services de police municipaux ont également pris des mesures importantes. Il convient notamment de souligner qu'en 2022, la Commission de services policiers de Toronto a adopté une « politique relative à l'utilisation des technologies d'intelligence artificielle » (« Politique sur l'IA de la CSPT »)³⁹. Plusieurs autres services de police de l'Ontario ont adopté des politiques relatives à l'IA à portée limitée, notamment ceux de Peel, de Durham, de York et d'Ottawa.

Les consultations menées par la CDO confirment que de nombreux autres services policiers et commissions de police canadiens envisagent d'adopter des politiques en matière d'IA responsable, qu'elles soient générales ou spécifiques à certaines technologies. La CDO a été impressionnée par l'engagement et la complexité de ces initiatives. Elle tient notamment à souligner le rôle de chef de file joué par l'Association canadienne des chefs de police (ACCP). En 2025-2026, l'ACCP a cherché à élaborer un cadre d'orientation en matière d'IA et un outil d'évaluation des risques liés à l'IA adaptés au contexte canadien. Une version préliminaire du modèle de l'ACCP a été approuvée en août 2026.

Commissaires à la protection de la vie privée

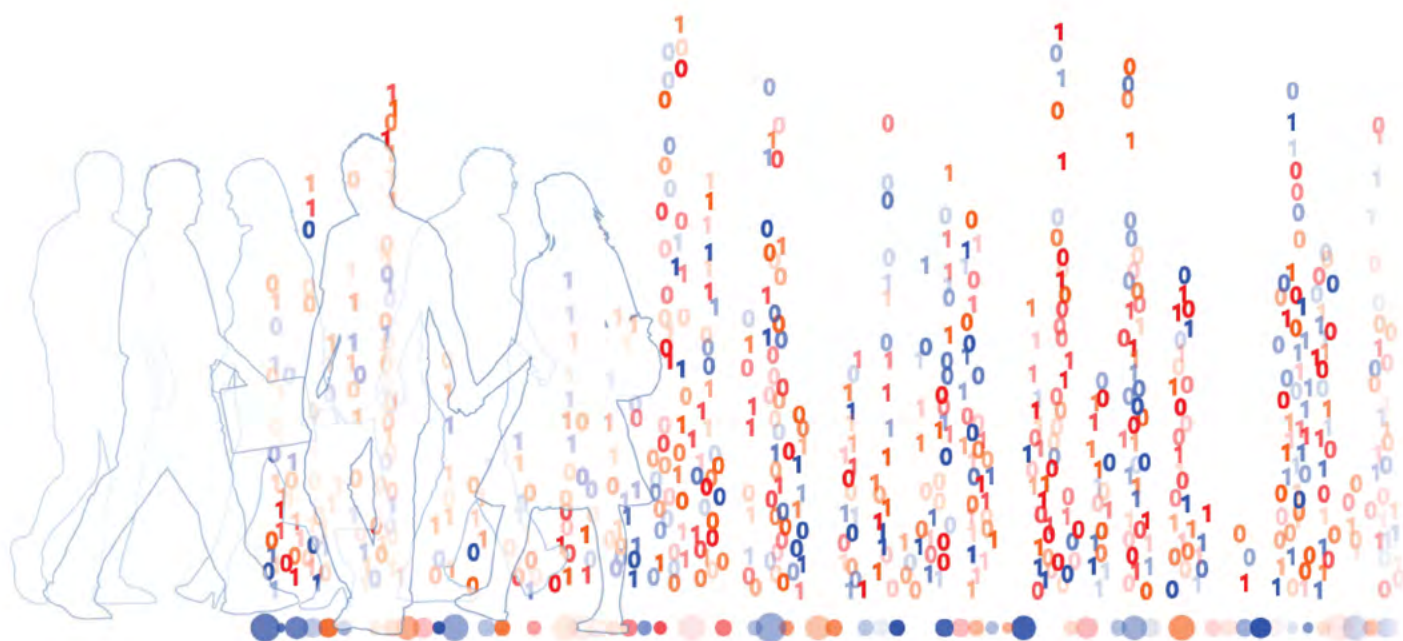
Les commissaires à la protection de la vie privée du Canada ont joué un rôle de premier plan et déterminant dans la promotion d'une IA responsable au Canada. À ce jour, les commissaires à la protection de la vie privée ont mené au moins six enquêtes, rapports ou documents d'orientation sur la RF et d'autres questions liées à l'IA dans les services de police canadiens.

Tribunaux

L'évolution la plus marquante en matière de politique judiciaire relative à l'IA responsable au Canada est le projet d'une nouvelle règle de procédure civile en Ontario. En 2025 et 2026, le sous-comité sur l'intelligence artificielle du Comité des règles civiles de l'Ontario (« sous-comité des règles civiles ») a proposé une nouvelle règle régissant les preuves issues de l'IA dans les procédures civiles en Ontario. De nombreuses personnes consultées considèrent que cette règle pourrait constituer un précédent important pour l'élaboration de règles dans le domaine de la justice pénale.

Autres institutions de la justice pénale

Outre les services policiers, les commissaires à la protection de la vie privée et les tribunaux, de nombreux autres ministères, conseils, organismes et organisations peuvent être appelés à utiliser ou à réglementer des systèmes d'IA, ou à trancher des litiges les concernant, dans le système de justice pénale de l'Ontario. La CDO constate que bon nombre de ces organismes se penchent activement, d'une manière ou d'une autre, sur les questions liées à l'IA dans le secteur pénal. Au mois d'août 2026, toutefois, le nombre de rapports publics ou de politiques traitant de ces questions émanant de ces institutions reste très limité.





Lacunes, risques et opportunités au sein du système de justice pénale canadien

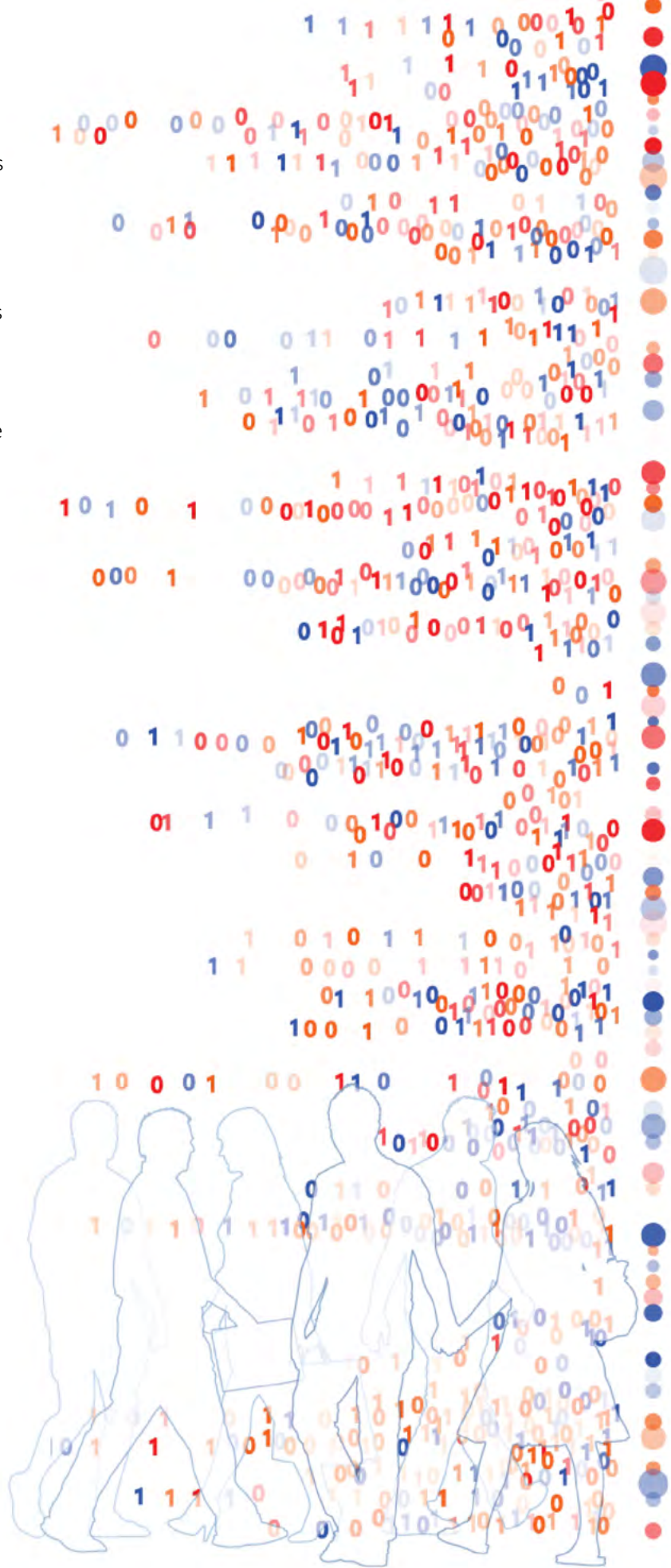
La section 5 du rapport final résume l'analyse par la CDO du cadre juridique et réglementaire visant les systèmes d'IA dans le secteur pénal provincial. Nos recherches et nos consultations confirment qu'il y existe encore des lacunes importantes et lourdes de conséquences en Ontario. On peut citer les exemples suivants :

- Absence de stratégie nationale ou régionale en matière d'IA dans le secteur pénal.
- Absence d'exigences obligatoires et cohérentes en matière de divulgation.
- Interdictions inexistantes ou incohérentes relatives à l'IA dans le secteur pénal, aux « barrières de protection » et aux critères de risque.
- Absence d'études d'impact spécifiques à l'IA dans le secteur pénal.
- Garanties procédurales pénales inexistantes, incohérentes ou imprécises.
- Absence d'obligation systématique de tester, d'auditer ou d'évaluer les systèmes d'IA dans le secteur pénal.
- Absence d'obligation systématique de mener des consultations publiques.

Ces lacunes s'aggraveront considérablement si d'autres services policiers et institutions de la justice pénale de l'Ontario adoptent l'IA. Il en résultera des risques juridiques inacceptables, des lacunes, des obstacles à une adoption responsable de l'IA et des occasions manquées d'améliorer la sécurité publique.

L'absence de réglementation des systèmes d'IA utilisés dans le secteur pénal pourrait entraîner l'utilisation, en Ontario, de technologies telles que la RF, la LIPA, le maintien de l'ordre prédictif et d'autres technologies, sans « barrières de protection » appropriées ni exigences en matière de responsabilité. Les préjudices potentiels pour les personnes accusées d'infractions criminelles, les tribunaux pénaux et la confiance du public sont prévisibles et considérables. L'absence d'obligations cohérentes en matière de divulgation, de biais ou d'évaluation des risques liés à l'IA signifie que les forces de l'ordre, les pouvoirs publics, les avocats et les tribunaux auront plus de mal à déterminer les utilisations appropriées et les limites des systèmes d'IA utilisés dans le secteur pénal.

Malgré cette analyse, il y a de nombreuses raisons d'être optimiste. La CDO a constaté un désir quasi unanime, parmi les acteurs du système de justice pénale, d'adopter une stratégie proactive et collaborative pour traiter les questions de gouvernance de l'IA dans le secteur pénal au Canada. Les consultations menées par la CDO ont également révélé un large consensus sur un ensemble de principes fondamentaux visant à garantir une IA responsable au Canada. Une autre conclusion importante concerne l'ampleur et la diversité des organisations et des personnes qui collaborent déjà sur les questions liées à l'IA dans le secteur pénal. Au Canada, la « communauté de pratique » dans ce domaine ne cesse de gagner en complexité et en nombre, car de plus en plus d'institutions, de chercheurs et d'intervenants s'intéressent à ces questions importantes.





Recommandations de la CDO

Ce projet est le premier au Canada à analyser les systèmes d'IA et les enjeux connexes tout au long du « cycle de vie » de la justice pénale. Il s'agit également du premier projet au Canada à mobiliser les parties prenantes et les institutions de l'ensemble du système de justice pénale afin d'élaborer conjointement des recommandations en vue d'une réforme législative, réglementaire et politique. Il en résulte un programme et un cadre complets visant à intégrer des principes et des politiques d'IA responsable dans l'ensemble du système de justice pénale. L'une des principales conclusions de ce projet est le désir quasi unanime des acteurs de la justice pénale de travailler ensemble pour aborder de manière constructive les enjeux liés à l'IA dans ce domaine.

Les 29 recommandations de la CDO sont fondées sur des principes solides, équilibrés et éprouvés. Elles s'appuient sur des précédents, des pratiques et des stratégies déjà en vigueur au Canada ou dans d'autres pays, ou encore en cours d'élaboration par les forces de l'ordre, les pouvoirs publics ou d'autres institutions judiciaires canadiennes.

Le texte intégral des recommandations du projet de la CDO sur l'IA dans le système de justice pénale est disponible [ici](#).

Recommandations n^{os} 1 à 3 : cadre provincial pour l'IA dans le système de justice pénale

Les recommandations n^{os} 1 à 3 de la CDO engageraient l'Ontario à mettre en place une gouvernance globale et responsable de l'IA dans le secteur pénal et confirmeraient les éléments clés nécessaires à sa mise en œuvre, notamment :

- une obligation de divulguer publiquement les systèmes d'IA utilisés en justice pénale ;
- des critères de risque recensant les utilisations interdites, à risque élevé, à usage restreint et à faible risque ;
- une obligation de mener une étude d'impact spécifique ;
- une obligation d'évaluer les systèmes d'IA utilisés en justice pénale au regard du droit canadien, ainsi que de vérifier leur compétence légale en matière d'autorité et de finalité ;
- des garanties procédurales ;
- un soutien aux pilotes d'IA en matière de justice pénale ;
- des exigences obligatoires et permanentes en matière d'audit et d'évaluation ;

- des normes et des politiques d’approvisionnement régissant les pratiques responsables en matière de logiciels;
- un organisme de surveillance indépendant;
- des garanties relatives à l’indépendance judiciaire et au privilège de non-divulgaration dans le cadre d’une enquête.

Un cadre provincial favorisera une adoption responsable de l’IA en matière pénale dans tout l’Ontario, améliorera la capacité de la province à promouvoir, à évaluer et à superviser les systèmes d’IA et mettra en place un programme provincial transparent et complet.

Recommandation n° 4 : législation provinciale sur l’IA en matière de justice pénale

La recommandation n° 4 de la CDO vise à modifier la [*Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique*](#) de l’Ontario ou à créer une législation complémentaire établissant des exigences strictes en matière de responsabilité des systèmes d’IA dans le secteur pénal, notamment :

- un principe de précaution;
- le devoir de donner la priorité au respect des droits, de la législation et des valeurs fondamentales du Canada;
- des catégories de risque obligatoires;
- la divulgation publique, l’évaluation des risques, les garanties juridiques et les exigences en matière d’audit.

La recommandation n° 4 traite de la nécessité d’assurer une cohérence au niveau provincial et de définir des exigences de base. La législation provinciale apportera cohérence et coordination à ce qui est actuellement un réseau décentralisé et désorganisé. Le besoin de coordination provinciale se fait de plus en plus pressant, à mesure que de plus en plus de services de police ontariens et d’autres institutions commencent à utiliser l’IA.

La recommandation n° 4 établit également des règles de gouvernance tenant compte des droits judiciaires et des risques en jeu. L’utilisation de l’IA dans le système de justice pénale touche certains des enjeux et droits les plus importants de la société canadienne, notamment la sécurité publique, la liberté individuelle, les droits garantis par la *Charte*, les droits procéduraux, ainsi que la confiance du public dans des institutions clés, notamment les tribunaux et les forces de l’ordre.

La CDO souligne que l’IA dans le système de justice pénale doit faire l’objet d’une réglementation exhaustive, non seulement en raison de l’étendue et de la gravité des risques juridiques, mais aussi en raison de l’ampleur potentielle de ces risques. En termes simples, le nombre de personnes dont les droits pourraient être affectés par les systèmes d’IA dans le secteur pénal dépasse de loin l’ampleur et l’impact des techniques d’enquête policière traditionnelles.

Heureusement, l’Ontario a déjà créé un précédent en adoptant une législation-cadre sur l’IA. La *LRSCN* confère à la province le pouvoir de réglementer l’utilisation de l’IA dans la majeure partie du secteur public de l’Ontario. La recommandation n° 4 instaurerait un cadre législatif de gouvernance de l’IA dans le domaine de la justice pénale. En effet, il serait déconcertant que l’IA utilisée dans les écoles publiques soit soumise à cette législation, mais pas les systèmes de justice pénale, qui présentent les risques les plus élevés.

Il existe de nombreux précédents internationaux en matière d’élaboration de cadre législatif visant à réglementer les systèmes d’IA.

La recommandation n° 4 inclut également un principe de précaution et l’obligation d’évaluer de façon prioritaire la conformité des systèmes d’IA dans le secteur pénal avec le droit pénal canadien. Ces dispositions, prises ensemble, garantiraient qu’aucun système d’IA à risque élevé ou à usage restreint ne soit déployé avant d’avoir subi une évaluation préalable des risques d’atteinte aux droits individuels et des implications systémiques découlant de l’absence de barrières de protection inhérentes aux principes fondamentaux d’équité procédurale et du droit de la preuve.

En 2025-2026, l'ACCP a cherché à élaborer un cadre d'orientation en matière d'IA et un outil d'évaluation des risques liés à l'IA adaptés au contexte canadien. Une version préliminaire du modèle de l'ACCP a été approuvée en août 2026. Il est important de noter que cette version préliminaire reprend les principales recommandations de la CDO, notamment :

- adopter le principe de précaution;
- évaluer l'IA à l'aide de quatre catégories de risque standard (y compris les interdictions relatives à l'IA);
- donner la priorité à la légalité et aux droits fondamentaux en tant que critère principal d'évaluation de l'IA.

Recommandations n^{os} 5 à 7 : déclaration provinciale et surveillance

Les recommandations n^{os} 5, 6 et 7 de la CDO établissent un régime provincial efficace de déclaration et de surveillance de l'IA en matière pénale. Ces recommandations favorisent une gouvernance de l'IA en matière pénale fondée sur des données probantes. Elles soutiennent également l'adoption responsable de l'IA, ainsi que la confiance du public et la reddition de comptes.

Il existe en Ontario de nombreuses lois, réglementations et politiques visant à garantir la publication d'informations et la transparence dans le domaine de l'application de la loi au niveau provincial, notamment la *Loi de 2019 sur la sécurité communautaire et les services policiers*. Ces dispositions sont essentielles à une bonne gouvernance, à un contrôle efficace et à la confiance du public dans les forces de l'ordre, en particulier dans les contextes à haut risque. Les obligations de déclaration à l'échelle de la province favorisent également l'élaboration de rapports, de règles et de mesures d'application cohérents, exhaustifs et fondés sur des données probantes.

À l'heure actuelle, il n'existe aucune communication publique et exhaustive sur la manière dont les organismes provinciaux chargés de la justice pénale utilisent l'IA, sur les avantages et les répercussions que peut avoir cette utilisation ni sur la rentabilité de ces systèmes ou leur capacité à atteindre leurs objectifs.

Les recommandations n^{os} 5, 6 et 7 définissent les infrastructures essentielles pour la mise en place d'un régime efficace de déclaration visant l'IA en matière pénale et de reddition de comptes au public en Ontario.

La recommandation n^o 5 prévoit de centraliser l'expertise en matière d'IA dans le domaine pénal au sein de deux organismes de surveillance indépendants : l'inspecteur général des services policiers et l'Agence des plaintes contre les forces de l'ordre de l'Ontario. Cela permettra de renforcer leur capacité à superviser les systèmes d'IA, à enquêter sur les plaintes et à rendre compte des problèmes systémiques.

La recommandation n^o 5 constitue une mesure provisoire. Elle anticipe la recommandation n^o 6, qui habiliterait la création d'une autorité de surveillance provinciale dédiée aux systèmes d'IA dans le secteur pénal, comme évoqué dans la recommandation n^o 19.

La recommandation n^o 7 soutient ces objectifs en obligeant les services chargés de l'application de la loi à mettre en place des politiques spécifiques en matière de gouvernance et d'exploitation de l'IA, et à désigner des responsables chargés de la mise en œuvre de ces politiques.

Recommandation n° 8 : souveraineté numérique et approvisionnement

La recommandation n° 8 de la CDO protégerait la souveraineté numérique des systèmes d'IA dans le secteur pénal en Ontario. Elle instaurerait également un pouvoir législatif permettant de règlementer les clauses types des contrats avec des fournisseurs tiers d'IA.

Cette recommandation est nécessaire pour garantir que les systèmes d'IA utilisés par les institutions provinciales de la justice pénale répondent à des normes cohérentes et applicables, pour assurer une gestion adéquate des données et pour respecter la législation canadienne en matière de protection de la vie privée ainsi que les autres lois en vigueur. D'autres dispositions sont examinées dans la recommandation 18.

Recommandation n° 9 : engagement civique

La recommandation n° 9 de la CDO établit le fondement juridique permettant de prévoir une série de mesures en matière d'engagement civique et de transparence, notamment la participation du public à tout processus d'évaluation de l'IA, la publication de déclarations annuelles sur l'utilisation des systèmes d'IA, la participation du public au sein de l'autorité de surveillance provinciale, ainsi que des révisions législatives obligatoires.

Recommandations n°s 10 à 15 : gestion des risques des systèmes d'IA en matière de justice pénale

Les recommandations n°s 10 à 15 de la CDO établissent un cadre de gestion des risques pour gouverner l'utilisation des systèmes d'IA dans le secteur pénal en Ontario. Ces recommandations :

- indiquent quatre catégories de risque qui devraient être définies dans la législation, y compris les interdictions;
- demandent à la province d'organiser des consultations publiques sur les questions liées à la gestion des risques;
- identifient les critères potentiels, les cas d'utilisation et les mesures d'atténuation pour chaque catégorie de risques.

Les recommandations de la CDO reflètent plusieurs principes et objectifs qui ont recueilli un large soutien lors de nos consultations, notamment :

- la nécessité de règlementer les systèmes d'IA dans le secteur pénal en fonction des risques;
- la priorité d'identifier et d'atténuer les risques liés aux systèmes d'IA dans le secteur pénal à incidence élevée;
- la gestion des risques favorisant une utilisation responsable de l'IA dans le secteur pénal, la responsabilité juridique et la confiance du public;
- des catégories de gestion des risques obligatoires et cohérentes;
- des niveaux de risque et leur évaluation qui s'appuient sur le droit pénal canadien;
- la nécessité de réduire les chevauchements et d'assurer la cohérence et l'interopérabilité entre les organisations;
- la gestion des risques qui s'appuie sur une expertise centralisée, un suivi et une certification;
- la nécessité d'avoir la participation du public.

Les recommandations n°s 10 et 11 définissent les principes fondamentaux ou les conditions préalables de ce cadre. Les recommandations n°s 12 à 15 traitent de questions spécifiques.

La recommandation n° 10 prévoit la mise en place de quatre catégories de risques liés à l'IA en droit pénal : « interdits », « à risque élevé », « à usage restreint » et « à faible risque ». Ces catégories sont conformes aux catégories de risques définies dans le règlement de l'UE sur l'IA ainsi que dans d'autres législations et cadres internationaux. Elles s'alignent également sur les catégories de risques liés à l'IA déjà établies au Canada, notamment celles figurant dans la directive fédérale relative aux PDA, la LRSCN et, surtout, la politique de la Commission de services policiers de Toronto sur l'utilisation de l'IA⁴⁰.

Ces catégories ont reçu un large soutien lors de nos consultations, car elles reflètent une échelle progressive appropriée des capacités des systèmes d'IA dans le secteur pénal, des risques associés et des mesures d'atténuation. Elles ont récemment été adoptées dans un projet de cadre d'orientation sur l'IA élaboré par l'Association canadienne des chefs de police.

Il est essentiel d'organiser des consultations publiques et d'impliquer la population sur ces questions, en particulier en ce qui concerne les systèmes d'IA à risque élevé dans le secteur pénal, tels que la RF ou le maintien de l'ordre prédictif, qui suscitent beaucoup de scepticisme dans le public. C'est pourquoi la recommandation n° 11 engage la province à mener des consultations publiques sur les questions importantes relatives à la gestion des risques liés à l'IA.

Recommandations n°s 12 à 15 : critères de risque, pratiques et mesures d'atténuation

D'une manière générale, les recommandations n° 12 à 15 précisent chacune des quatre catégories définies dans la recommandation n° 10. Plus précisément, les recommandations n° 12 à 15 identifient 1) les critères ou cas d'utilisation permettant de déterminer si un système d'IA dans le secteur pénal doit être interdit ou considéré comme présentant un risque élevé, soumis à des restrictions ou présentant un risque faible et 2) les mesures visant à atténuer ce risque.

La CDO est convaincue que les recommandations n° 12 à 15 sont cohérentes et fondées. Les recommandations reflètent une combinaison de normes et de pratiques actuelles ou émergentes en matière de gouvernance responsable de l'IA dans le domaine pénal, tant au Canada qu'à l'échelle internationale. Cela dit, ces recommandations privilégient l'ouverture et l'intégration plutôt qu'une conclusion définitive. La CDO recommande la tenue de consultations provinciales afin de garantir une prise de décision optimale et de promouvoir la responsabilité publique et la confiance.

Recommandation n° 12 : systèmes d'IA interdits

Les interdictions et les « limites » en matière d'IA constituent sans doute la stratégie la plus déterminante et la plus médiatisée pour instaurer la confiance dans les systèmes d'IA et réduire les risques liés à cette technologie. Par exemple, les limites ou les interdictions concernant l'utilisation par la police de la RF en temps réel pourraient réduire considérablement les risques liés à la surveillance de masse rendue possible par la RF, au contrôle policier excessif des communautés racisées et aux violations massives de la vie privée.

À l'échelle internationale, de nombreux gouvernements ont adopté ou proposé des interdictions visant certaines technologies d'IA en droit pénal ou leur utilisation dans des circonstances spécifiques, notamment le règlement de l'UE sur l'IA.

L'exemple canadien le plus significatif en matière d'interdictions et de « limites » concernant l'IA dans le domaine policier est la politique de la Commission de services policiers de Toronto relative à l'utilisation de l'IA. Cette politique recense un large éventail de « technologies à risque extrême » interdites, dont « l'adoption ne peut être envisagée ». On peut citer les exemples suivants :

1. Toute application dans laquelle il n'y a pas d'« intervention humaine » qualifiée.
2. Lorsque l'utilisation de l'application entraîne une surveillance de masse, définie comme la surveillance d'une population ou d'une partie importante de celle-ci, ou l'analyse de données collectées de façon arbitraire sur une population ou une grande partie de celle-ci.
3. Toute application de l'IA dans une situation mettant en jeu la sécurité des personnes, c.-à-d. une application dans laquelle l'intervention de la technologie d'IA pourrait ralentir le temps de réaction de l'intervenant humain, entraînant ainsi un risque pour la vie de membres du public ou des forces de l'ordre.
4. Toute application dont on sait ou dont on peut raisonnablement supposer qu'elle causera un préjudice ou aura une incidence sur les droits d'un individu, malgré l'utilisation de techniques d'atténuation, en raison de biais ou d'autres défauts.
5. Toute application utilisée pour prédire ou attribuer une probabilité qu'un individu ou un groupe d'individus commette une infraction ou récidive.
6. Toute application utilisant des données recueillies conformément à la politique de la CSPT intitulée *Regulated Interaction with the Community and the Collection of Identifying Information* (Interactions réglementées avec la collectivité et collecte de renseignements identificatoires) ou les données historiques sur les interactions avec la police telle que définie dans cette politique.
7. Lorsque des données d'entraînement ou de transaction sont connues ou présumées provenir d'une source illégale, ou lorsqu'elles proviennent d'une source inconnue⁴¹.

Le pouvoir d'interdire par voie législative certains types de systèmes d'IA est également prévu par la *LRSCN* de l'Ontario⁴².

Recommandation n° 13 : systèmes d'IA à risque élevé

La recommandation n° 13 définit les critères et pratiques proposés pour identifier les systèmes d'IA « à risque élevé » dans le secteur pénal. Ces systèmes ne seraient pas interdits, mais soumis à des mesures d'atténuation exhaustives, qui sont également décrites dans la recommandation.

Selon la CDO, les systèmes d'IA devraient être considérés comme « à risque élevé » lorsqu'ils présentent des risques et des répercussions prévisibles sur les droits et libertés fondamentaux, y compris les droits judiciaires garantis par la *Charte*, la common law régissant le droit criminel, le droit de la preuve, l'équité procédurale, ainsi que les droits de la personne et le droit à la vie privée.

La politique sur l'IA de la CSPT comprend plusieurs exemples de « technologies à risque élevé » désignées à titre préventif, ce qui les soumet à des exigences de contrôle plus strictes, notamment :

1. lorsque les données d'entraînement ou de transaction sont identifiées ou considérées comme étant de mauvaise qualité, comportant des biais, ou lorsque la qualité de ces données est inconnue;
2. lorsque les données d'entraînement peuvent être influencées ou biaisées par des acteurs malveillants;
3. les applications qui associent des données biométriques à des renseignements personnels (p. ex., la reconnaissance faciale);
4. lorsque le système proposé pourrait être utilisé pour faciliter l'identification de personnes en vue de leur arrestation, leur détention ou leur interrogatoire;
5. lorsque le processus impliqué suggère une affectation de ressources policières;

6. lorsqu'un système qui, par ailleurs, mériterait une évaluation de risque modérée ne fait pas l'objet d'une validation indépendante;
7. lorsqu'un système ne peut pas être entièrement explicable dans son fonctionnement⁴³.

Le chapitre III du règlement de l'UE sur l'IA classe également plusieurs systèmes d'IA dans le secteur pénal comme « à haut risque » en raison du risque important qu'ils font peser sur les droits et libertés⁴⁴.

La liste des systèmes d'IA à risque élevé proposée dans la recommandation n° 13 tient compte des applications concrètes de l'IA qui suscitent des inquiétudes au Canada et dans le monde entier.

Le rôle des dérogations, des situations d'urgence et des circonstances exceptionnelles

Il a été question, dans les consultations menées par la CDO, du rôle des dérogations, des situations d'urgence et des circonstances exceptionnelles dans le cadre des catégories d'évaluation « interdites » et « à risque élevé ». La CDO n'a formulé aucune recommandation sur ces questions dans le rapport final.

Recommandation nos 14 et 15 : utilisation restreinte/technologies à risque moyen et à faible risque

La recommandation n° 14 décrit les critères et pratiques proposés pour identifier les systèmes d'IA « à usage restreint » dans le secteur pénal. Ces systèmes ne seraient ni « interdits » ni « à risque élevé », mais seraient soumis à des mesures d'atténuation exhaustives, qui sont également décrites dans la recommandation.

Selon la CDO, les systèmes d'IA devraient être considérés comme relevant d'un « usage restreint » lorsqu'ils présentent des risques d'effets négatifs sur les individus ou la société, qu'ils portent atteinte à l'administration de la justice ou qu'ils sont susceptibles de compromettre la confiance du public dans le système de justice pénale.

La recommandation n° 15 propose des critères permettant d'identifier les systèmes d'IA « à faible risque » comme étant ceux qui ne présentent aucun risque d'atteinte aux droits fondamentaux, d'impacts négatifs sur les individus ou la société, de préjudice à l'administration de la justice, ni de compromettre la confiance du public dans le système de justice pénale. Les systèmes « à faible risque » accomplissent une tâche procédurale ou préparatoire étroite, n'influencent pas de manière significative ni ne remplacent le résultat d'une évaluation ou d'une prise de décision, et sont facilement corrigibles ou réversibles.

Recommandation n° 16 : registre public des systèmes d'IA dans le secteur pénal

La recommandation n° 16 prévoit la création d'un registre public exhaustif des systèmes d'IA utilisés dans le système de justice pénale de l'Ontario. Elle précise les renseignements essentiels à y inclure et impose des obligations régulières en matière de déclaration.

Recommandations nos 17 et 18 : évaluations des risques

La recommandation n° 17 engage le gouvernement de l'Ontario à impliquer les institutions de la justice pénale dans l'élaboration d'un outil standardisé d'évaluation des risques liés à l'IA dans le domaine pénal. Des critères, des catégories et des mesures d'atténuation communs en matière d'évaluation des risques garantiraient une approche cohérente pour une utilisation fiable de l'IA au sein des différentes institutions de la justice pénale.

La recommandation n° 18 établit le cadre législatif permettant de définir des normes pour les projets pilotes d'IA et les évaluations de performance en conditions réelles; un ensemble de normes en matière d'approvisionnement et de clauses types de contrats avec les fournisseurs, ainsi que des mesures de protection de la souveraineté numérique.

Recommandations n^{os} 19 et 20 : surveillance et déclarations

Les recommandations n^{os} 19 et 20 de la CDO énoncent des obligations détaillées en matière de surveillance et de déclaration. Ces recommandations comportent deux volets : d'une part, elles engageraient la province à mettre en place un organisme chargé de surveiller les systèmes d'IA dans le domaine de la justice pénale. Les parties prenantes estimaient qu'une autorité de surveillance de l'IA dans le système de justice pénale pourrait centraliser l'expertise, éliminer les évaluations en double, certifier les technologies d'IA destinées à être utilisées à l'échelle provinciale, assurer un suivi continu des évolutions technologiques, fournir des témoins experts indépendants en matière d'IA ainsi que des avis d'experts indépendants, et favoriser la reddition de comptes au public et la participation de celui-ci. Dans l'intervalle, les recommandations ajoutent des responsabilités de déclaration, de surveillance et de consultation aux fonctions de l'inspecteur général des services policiers de l'Ontario, de l'Agence ontarienne des plaintes contre les forces de l'ordre et d'autres organismes.

Recommandations n^{os} 21 à 24 : preuves issues de l'IA

Les recommandations n^{os} 21 à 24 de la CDO portent sur les éléments de preuve créés ou optimisés par l'IA, susceptibles d'être utilisés dans le cadre d'une procédure pénale ou pendant une enquête criminelle. Ces recommandations tiennent compte à la fois du partage des compétences en la matière entre le gouvernement provincial, le gouvernement fédéral et divers comités chargés des règles de procédure, et de la nécessité d'élaborer des règles de preuve spécifiques pour les différentes étapes du processus de justice pénale.

La CDO et les parties prenantes s'accordent à dire que les éléments de preuve issus de l'IA peuvent apporter un bénéfice considérable aux enquêtes policières, réduire les dépenses et renforcer la sécurité publique. En même temps, les outils d'IA et les éléments de

preuve issus de l'IA comportent également des risques potentiellement graves. L'analyse de la CDO porte sur deux catégories émergentes d'éléments de preuve issus de l'IA : 1) les éléments de preuves reconnus en matière d'IA et 2) les éléments de preuves non reconnus en matière d'IA, y compris la technologie d'hypertrucage.

Parmi les exemples de preuves reconnues en matière d'IA, on peut citer les suivants :

- Outils d'IA autorisés à des fins d'enquête.
- Assistants d'IA utilisés pour transcrire ou décrire des fichiers vidéo et audio, ainsi que pour rédiger des rapports d'incident de police.
- Outils d'IA destinés à la recherche juridique et à la rédaction de documents juridiques.

Voici quelques exemples de preuves non reconnues en matière d'IA :

- Les enquêtes policières qui reçoivent de tiers des preuves peu fiables issues de la technologie d'hypertrucage.
- Les agents de police qui utilisent des outils d'IA non autorisés, mais accessibles au public, tels que des applications de géolocalisation et de reconnaissance faciale, ou qui s'appuient sur des renseignements recueillis par des systèmes de surveillance présentant un risque de discrimination et de biais.
- Les images ou vidéos brutes « améliorées » artificiellement par un système d'IA qui, loin de restituer les détails, les déduit ou les ajoute, ce qui compromet la fiabilité et la validité des preuves.
- Des documents rédigés, modifiés ou corrigés à l'aide de l'IA – tels que des notes de police et des rapports d'incident, des résumés de documents ou des transcriptions et descriptions audio et vidéo – susceptibles de contenir des erreurs hallucinées ou fallacieuses.

Les personnes consultées ont généralement convenu que les données relatives à l'IA soulèvent les questions suivantes :

- Les outils d'IA sont très récents. De ce fait, la police, les procureurs, les avocats de la défense et les tribunaux doivent se pencher sur des questions nouvelles et complexes concernant la fiabilité, la validité et les biais des preuves issues de l'IA.
- Dans de nombreux cas, il semble que l'intervenant humain chargé des preuves issues de l'IA ne dispose pas de la formation, des ressources ou de l'indépendance nécessaires pour évaluer correctement le système.
- Il n'existe aucune obligation systématique de divulguer l'utilisation de l'IA ou le recours à des preuves issues de l'IA. Il n'y a pas non plus de clarté sur ce que devrait impliquer une telle divulgation.
- Les procédures où le seuil de preuve est moins élevé sont moins susceptibles de permettre un examen efficace des systèmes d'IA, en particulier les audiences de mise en liberté sous caution, où le rythme rapide, la forte pression et la charge probatoire réduite font qu'il est peu probable que les preuves issues de l'IA soient examinées de manière appropriée.
- L'accès à des experts en IA est difficile.
- Les tribunaux pourraient devoir examiner simultanément de nombreux outils d'IA différents.
- La judiciarisation des conflits a peu de chances d'être efficace.
- Les technologies d'hypertrucage constituent un problème émergent.

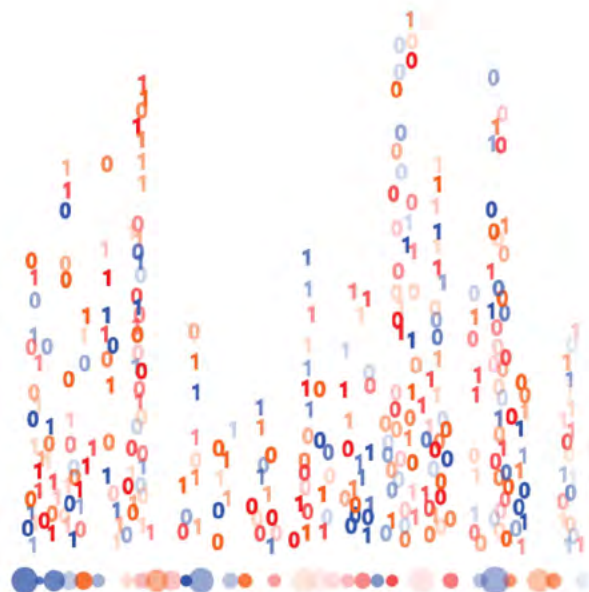
Les parties prenantes ont reconnu que le droit de la preuve pénale est souple et s'adapte régulièrement aux nouvelles technologies. Elles ont toutefois estimé que les dispositions existantes de la *Loi sur la preuve au Canada* et de la *Loi sur la preuve* de l'Ontario régissant les documents électroniques ou commerciaux n'étaient pas bien adaptées aux preuves issues de l'IA.

Compte tenu des questions susmentionnées, la CDO et les parties consultées ont globalement convenu que les preuves issues de l'IA devaient être reconnues comme une catégorie distincte de preuves, régie par un ensemble de règles et de procédures spécifiques dans le cadre de la justice pénale.

La CDO et les parties consultées ont par ailleurs convenu que les règles proposées en matière de preuve civile liée à l'IA en Ontario constituent un précédent important pour l'adoption de règles équivalentes dans le système de justice pénale. Ces règles auraient besoin d'être adaptées aux procédures pénales.

Pour remédier à ces problèmes, les recommandations n^{os} 21 à 23 formulent une série de propositions visant à créer des comités spécialisés chargés d'étudier et de formuler des recommandations sur des règles détaillées relatives à l'IA dans le cadre des procédures pénales. Ce travail devrait s'appuyer sur certaines exigences fondamentales, notamment une obligation de divulgation à différentes étapes de la procédure pénale (y compris les enquêtes sur le cautionnement) et la prise en compte des critères d'admissibilité, de fiabilité et de biais des preuves issues de l'IA.

La recommandation n^o 24 de la CDO propose que le ministère du Procureur général (MPG) modifie le manuel de poursuite de la Couronne en y intégrant des directives visant à mettre en œuvre les recommandations formulées ci-dessus.



Recommandations n^{os} 25 à 29 : accès à la justice et capacité du système

Les recommandations n^{os} 25 à 29 soulignent l'importance d'assurer aux personnes accusées d'infractions criminelles et à leurs avocats un accès réel à la justice lors d'instances criminelles impliquant l'utilisation de systèmes d'IA. Ces recommandations abordent également la nécessité de renforcer les capacités des cours provinciales pour qu'elles soient en mesure de répondre efficacement aux défis anticipés dans l'utilisation des systèmes d'IA, notamment la nécessité de pouvoir faire appel à des experts et à des outils d'analyse judiciaire.

Aide juridique Ontario

Les recommandations n^{os} 25 à 27 renforceraient les capacités nécessaires pour garantir que les personnes accusées d'infractions criminelles et leurs avocats aient un accès effectif à la justice et soient en mesure de présenter une défense pleine et entière face aux enquêtes menées à l'aide de l'IA.

La recommandation n° 25 engagerait le MPG à donner à Aide juridique Ontario (AJO) les fonds et les ressources nécessaires pour garantir que les avocats de la défense pénale soient en mesure de présenter une défense pleine et entière dans les dossiers impliquant des preuves issues de l'IA. La recommandation n° 26 prévoit la création d'un centre d'excellence en IA au sein d'AJO.

La recommandation n° 27 prévoit la création d'un comité consultatif externe dédié à l'AJO, chargé de se réunir régulièrement et de conseiller l'administration et la direction de l'AJO sur les questions relatives à l'IA.

Accès à des experts et à des outils d'analyse judiciaire

Les recommandations n^{os} 28 et 29 sont des recommandations transitoires. En attendant la création de l'autorité de surveillance de l'IA dans le secteur de la justice pénale proposée, ces recommandations préconisent que les ressources indispensables en matière de litiges soient mises à disposition plus rapidement par l'intermédiaire du Centre des sciences judiciaires (CSJ).

La recommandation n° 29 met l'accent sur deux initiatives importantes au sein du CSJ. Premièrement, le CSJ devrait mettre en place un programme accessible gratuitement aux avocats de la défense pénale qui souhaitent obtenir un avis sur la fiabilité, la validité et les biais des éléments de preuve issus de l'IA, des outils judiciaires et des pratiques d'enquête. Deuxièmement, le CSJ devrait mettre en place un programme de certification et de mise à disposition d'outils d'analyse judiciaire liés à l'IA à l'intention des avocats, tels que des plateformes permettant d'identifier les preuves et les documents hypertriqués.

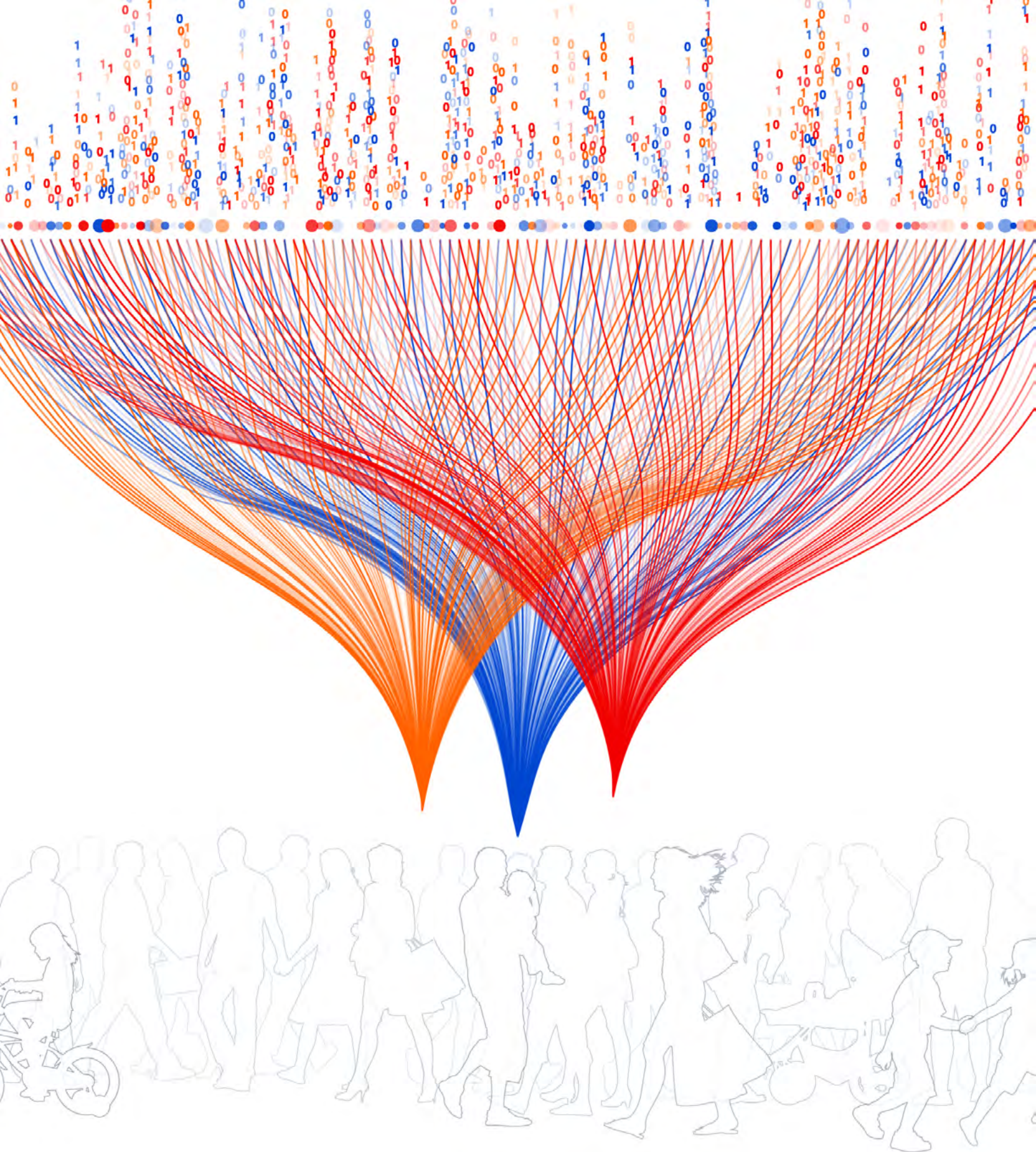


Endnotes

- 1 Parlement du Royaume-Uni, « Facial recognition technology in policing » [RF Parlement du R-U (8 avril 2026, en ligne : <https://post.parliament.uk/facial-recognition-technology-in-policing/>).
- 2 Voir, de manière générale, DeFlock, an American « open-source project mapping licence plate readers » [DeFlock], en ligne : <https://deflock.org/> (consulté le 14 septembre 2026).
- 3 Cette liste a été établie à partir de plusieurs sources, notamment Benjamin Perrin, Geoffrey Liew et Isabelle Sweeney, *AI et maintien de l'ordre : rapport de recherche sur la gouvernance et l'utilisation de l'IA par la police au Canada* (Initiative d'IA et de justice pénale UBC, 2026) [Rapport de l'UBC sur l'utilisation de l'IA par la police], en ligne : <https://benjaminperrin.ca/f/ai-policing-research-report-published>; les rapports sur l'IA en droit pénal de la CDO; divers renseignements médiatiques cités dans le présent rapport; Citizen Lab, « Algorithmic Policing in Canada Explained » (1^{er} septembre 2020), en ligne : <https://citizenlab.ca/research/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/algorithmic-policing-in-canada-explained/> et Ben Perrin, *Artificial Intelligence & Criminal Justice: Cases and Commentary* (mis à jour le 2 février 2026), en ligne : <https://canlii.ca/t/7njwh>.
- 4 Voir la section 2 du rapport final de la Commission du droit de l'Ontario sur l'IA dans le système de justice pénale et ses recommandations [rapport final de la CDO sur l'IA dans le système de justice pénale] (2026), en ligne : <https://lco-cdo.org/fr/projets/ia-dans-le-systeme-de-justice-penale/> pour une analyse approfondie de ces questions.
- 5 Voir l'encadré « How FRT is Used in the UK » dans la section 2 du rapport final de la CDO sur l'IA dans le système de justice pénale pour en savoir plus.
- 6 Selon l'« Atlas of Surveillance », un projet de recherche d'origine source ouverte mené par l'Electronic Frontier Foundation, il pourrait y avoir jusqu'à 980 sites ou applications de RF au sein de divers services de police et agences gouvernementales à travers les États-Unis en septembre 2026 [Atlas of Surveillance], en ligne : <https://atlasofsurveillance.org/atlas>.
- 7 Rapport de l'UBC sur l'utilisation de l'IA par la police, p. 14.
- 8 Office of the Inspector General of the Los Angeles Police Commission, *LAPD Review of the Department's ALPR System and Use in the Field* (10 juillet 2026) [LAPD ALPR Report] p. 2, en ligne : <https://www.oig.lacity.org/audit-and-complaint-reports>.
- 9 Service de police de Toronto, « Automatic Licence Plate Recognition », en ligne : <https://www.tps.ca/use-technology/automatic-licence-plate-reader/> (consulté le 14 septembre 2026).
- 10 Voir la section 3 du rapport final de la CDO sur l'IA dans le système de justice pénale pour une analyse approfondie de ces questions.
- 11 Metropolitan Police, *Live Facial Recognition Annual Report*, [rapport du Met sur la reconnaissance faciale en direct] (2025), en ligne : <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology/>, à la p. 5.
- 12 David Freeman Engstrom et Daniel E. Ho, *Algorithmic Accountability in the Administrative State* ((2020) Yale J on Reg 800) p. 821, en ligne : <https://www.yalejreg.com/print/algorithmic-accountability-in-the-administrative-state/>.
- 13 Organisation internationale de police criminelle (INTERPOL), *Responsible AI Principles* (2024) [INTERPOL Responsible AI Principles] (2024), en ligne : <https://www.interpol.int/fr/Notre-action/Innovation/Manuel-d-utilisation-de-l-intelligence-artificielle> p. 13
- 14 Benjamin Perrin, Geoffrey Liew et Isabelle Sweeney, *IA et maintien de l'ordre : rapport de synthèse des connaissances sur la gouvernance et l'utilisation de l'intelligence artificielle par la police au Canada* (2026), en ligne : https://commons.allard.ubc.ca/fac_pubs/2834/ p. 1-2.
- 15 Voir la section 4 du rapport final de la CDO sur l'IA dans le système de justice pénale pour une analyse approfondie de ces questions.

- 16 Union européenne, *Législation sur l'IA (règlement (UE) 2024/1689 du Parlement européen et du Conseil européen établissant des règles harmonisées concernant l'intelligence artificielle (2024)* [Règlement de l'UE sur l'IA], en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32024R1689>. Pour un bon résumé de la législation sur l'IA de l'UE, lire la page Web de la Commission européenne au <https://digital-strategy.ec.europa.eu/fr/policies/regulatory-framework-ai>.
- 17 Règlement de l'UE sur l'IA, chapitre II, article 5, al. 1h).
- 18 Règlement de l'UE sur l'IA, chapitre II, article 5, al. 1d).
- 19 Voir : Règlement de l'UE sur l'IA, chapitre III, annexe III.
- 20 États-Unis, Bureau du président, décret 14110, « Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence » [décret 14110] (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>
- 21 La CDO peut fournir un recueil sur demande.
- 22 Airsight, « Drone Laws », en ligne : <https://www.airsight.com/learn/airspace-security/drone-laws-rules-and-regulations> (consulté en août 2026).
- 23 DeFlock, « City Council ».
- 24 CBS 12 News WPEC, « Governor DeSantis calls Flock license plate readers “out of control.” » [CBS 12 News] (26 août 2026), en ligne : <https://www.youtube.com/shorts/m1ltxEuS38>.
- 25 Jesus Jimenez et David Ovalle, « In Red States, Law-and-Order Republicans Turn Against Flock Cameras », New York Times, 5 sept. 2026, [NYT Red States], en ligne : <https://www.nytimes.com/2026/09/05/us/red-states-republicans-flock-cameras.html>.
- 26 Big Brother Watch, « Stop Facial Recognition », en ligne : <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/> (consulté le 14 septembre 2026).
- 27 Royaume-Uni, bureau du Premier ministre, *The King's Speech 2026: Background Briefing Notes* (13 mai 2026) p. 68-69.
- 28 Gouvernement du R-U, « PoliceAI to speed up investigations and fight crime » (10 juin 2026), en ligne : <https://www.gov.uk/government/news/policeai-to-speed-up-investigations-and-fight-crime>.
- 29 *Loi sur la mise en œuvre de la Charte du numérique ; 1^{re} session 44^e 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>.
- 30 Gouvernement du Canada, *Stratégie nationale en matière d'intelligence artificielle du Canada : L'IA pour tous* [Stratégie nationale en matière d'IA du Canada] (2026), en ligne : https://ised-isde.canada.ca/site/isde/fr/strategie-nationale-matiere-dintelligence-artificielle-canada-lia-pour-tous#_Toc68.
- 31 *Loi sur les médias sociaux sécuritaires*, projet de loi C-34, 1^{re} session, 45^e législature, 2026 (première lecture le 10 juin 2026).
- 32 *Loi visant à protéger la vie privée et les données des consommateurs*, projet de loi C-36, 1^{re} session, 45^e législature, 2026 (première lecture le 15 juin 2026).
- 33 Canada, *Directive sur la prise de décisions automatisée* [Canada, Directive sur la PDA], 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/prise-decisions-automatisee/evaluation-incidence-algorithmique.html>.
- 34 Registre de l'IA du gouvernement du Canada 747-760, consulté le 18 août 2026. En ligne : <https://ouvert.canada.ca/data/fr/dataset/fcbc0200-79ba-4fa4-94a6-00e32facea6b/resource/369f6f34-148a-42ed-b581-8c164e941a89>.
- 35 *Loi de 2024 visant à renforcer la sécurité et la confiance en matière de numérique*, L.O. 2024, chapitre 24 [LRSCN], en ligne : <https://www.ontario.ca/lois/loi/24e24>.
- 36 Gouvernement de l'Ontario, consultation sur une proposition de loi : *Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public*.

- 37 LRSCN aux par. 5(1-6), 6(2), 7, 8.
- 38 Gouvernement de l'Ontario, ministère des Services au public et aux entreprises et de l'Approvisionnement, *Directive sur l'utilisation responsable de l'IA*, 1^{er} décembre 2024 [Directive IA Ontario].
- 39 Service de police de Toronto, « Use of Artificial Intelligence Technology » (présenté le 28 février 2022, mis à jour le 11 janvier 2024), en ligne : <https://tpsb.ca/home/about/policies-by-laws/board-policies/use-of-artificial-intelligence-technology/> [Politique sur l'IA de la CSPT].
- 40 Politique sur l'IA de la CSPT.
- 41 Politique sur l'IA de la CSPT.
- 42 LRSCN par. 5 (6).
- 43 Politique sur l'IA de la CSPT.
- 44 Règlement de l'UE sur l'IA, chapitre III, annexe III.



Law Commission of
Ontario

Commission du droit
de l'Ontario

2030, édifice Ignat Kaneff
Faculté de droit Osgoode Hall, Université York
4700, rue Keele, Toronto ON Canada M3J 1P3