

# Recensement des pistes d'action pour une intégration responsable de l'intelligence artificielle en milieu de travail

Le présent document regroupe un ensemble de pratiques et de pistes d'action qu'il est possible d'adopter afin de favoriser une intégration et une utilisation responsables de l'intelligence artificielle en milieu de travail. Ces pistes d'action sont regroupées par phases de déploiement d'un système d'intelligence artificielle (IA). Ensemble, ces phases forment le cycle de vie complet d'un tel système, depuis son idée initiale jusqu'à sa mise hors service. Reprises de l'Organisation de coopération et de développement économiques (OCDE), il importe de considérer chacune de ces phases afin d'assurer une utilisation **responsable, sécuritaire et adaptée aux contextes organisationnels** d'un système d'IA. Pour plus de détails, le lecteur est invité à consulter le document *Agir à chaque étape du cycle de vie de l'IA : pratiques et pistes d'action pour une intégration en milieu de travail*.

## Phase 1

### PLANIFICATION ET CONCEPTION

#### Une stratégie d'IA alignée sur les objectifs de l'organisation

- Énoncer les objectifs poursuivis par l'IA au sein de l'organisation et préciser les liens avec la mission et les priorités de l'organisation.
- Examiner les usages envisagés au regard des droits et libertés de la personne et des principes de non-discrimination.
- Considérer les effets possibles de l'IA sur les conditions de travail notamment en ce qui concerne les protections prévues par la Loi sur les normes du travail.
- Porter attention aux effets potentiels sur la santé, la sécurité et le bien-être, dans une logique de prévention prévue par la Loi sur la santé et la sécurité du travail.
- Prévoir les transformations de l'organisation du travail et des rôles.
- Favoriser des pratiques transparentes en matière d'utilisation de l'IA.

#### Création d'un comité éthique ou désignation d'un référent en IA

- Mettre en place la forme la plus adaptée au contexte organisationnel.
- Favoriser la diversité des expertises et des points de vue dans les espaces de réflexion.
- Identifier les projets d'IA susceptibles de soulever des enjeux particuliers et nécessitant une attention accrue.
- S'assurer que les mécanismes internes (comité éthique ou référent IA) sont en lien direct avec les instances dirigeantes, afin de favoriser une coordination efficace.

#### Définition claire des responsabilités

- Identifier les différents acteurs impliqués aux diverses étapes du cycle de vie des systèmes d'IA.
- Clarifier les rôles liés à la prise de décision, à la supervision et au suivi des effets de l'IA.
- Porter attention aux situations où les responsabilités humaines pourraient devenir moins visibles en raison de l'automatisation.
- Consigner les rôles et responsabilités dans des politiques ou pratiques internes.
- Favoriser une compréhension partagée des responsabilités au sein des équipes concernées.
- S'assurer d'une cohérence entre la répartition des responsabilités et les mécanismes de gouvernance existants.

#### Dialogue social et concertation

- Choisir les mécanismes de concertation les plus appropriés au contexte organisationnel.
- Échanger sur les usages envisagés de l'IA et sur leurs effets possibles sur le travail.
- Porter attention aux préoccupations exprimées par les travailleuses, les travailleurs et leurs représentantes et représentants.
- Utiliser le dialogue comme levier pour identifier des besoins d'accompagnement ou de formation.
- S'appuyer sur les instances de dialogue existantes.
- Considérer la concertation comme un processus évolutif, appelé à se poursuivre dans le temps.

## Phases 2 et 3

### COLLECTE ET TRAITEMENT DES DONNÉES, CONSTRUCTION ET ADAPTATION DU OU DES MODÈLES

#### Gouvernance des données : qualité, traçabilité, anonymisation, chiffrement et contrôle d'accès

- Mettre en place des mécanismes de vérification de la qualité des données, afin de s'assurer qu'elles sont exactes, complètes et pertinentes pour les usages de l'IA.
- Assurer la traçabilité des données.
- Déployer des mesures de sécurité adaptées pour protéger les données contre les accès non autorisés, les pertes ou les fuites.
- Privilégier des techniques d'anonymisation lorsque pertinentes, afin de limiter les risques liés aux renseignements personnels.
- Utiliser des mécanismes de chiffrement pour sécuriser les données, tant lors de leur stockage que lors de leur transmission.
- Encadrer les accès aux données en définissant des droits d'accès adaptés aux rôles et responsabilités des personnes.

#### Respect des lois et des réglementations en matière de données personnelles et de surveillance

- Informer les personnes concernées sur les données collectées et les usages qui en sont faits.
- Limiter la collecte aux données nécessaires aux fins poursuivies.
- Obtenir un consentement, en particulier lorsqu'il s'agit de données sensibles.
- Mettre en place des mesures de sécurité appropriées.
- Mettre en place un processus de gestion des incidents de confidentialité.
- Permettre aux individus d'accéder aux renseignements qu'ils ont fournis, de les rectifier et d'en demander le retrait.
- Se renseigner sur les pratiques des fournisseurs et des partenaires technologiques afin de mieux comprendre leurs approches en matière de protection des données, de sécurité et de respect des cadres juridiques.

## Phase 4

### TEST, ÉVALUATION, VÉRIFICATION ET VALIDATION

#### Évaluation des risques pour la santé, la sécurité et les conditions de travail

Mener et maintenir une évaluation des risques liés à l'IA permet d'en apprécier de manière continue les effets sur

- la charge mentale et cognitive, lorsque l'IA modifie le rythme de travail, la complexité des tâches ou les attentes de performance;
- les risques psychosociaux;
- la sécurité physique, lorsque l'IA intervient dans des processus opérationnels, le contrôle d'équipements ou la gestion de tâches présentant des dangers physiques;
- la fiabilité des systèmes, en cas de résultats inexacts, de défaillances techniques ou de décisions automatisées mal interprétées;
- l'organisation du travail, comme la redéfinition des tâches, l'intensification du travail ou la modification des responsabilités;
- les possibilités d'intégrer les risques liés à l'IA aux programmes de prévention existants ou d'ajuster le contenu de ces programmes, afin de tenir compte des nouveaux risques identifiés, conformément aux principes de prévention prévus par la Loi sur la santé et la sécurité du travail.

#### Contrôle et audit des risques pour la santé et la sécurité du travail

Il peut être utile de structurer les pratiques de suivi et de vérification afin de mieux appréhender leurs effets dans le temps en intégrant

- les modalités de suivi dans le temps des usages réels des systèmes d'IA et de leurs effets sur la santé et la sécurité;
- la capacité à prévenir l'apparition de biais discriminatoires ou d'effets non prévus sur la santé, la sécurité ou le bien-être des travailleuses et des travailleurs;
- la robustesse et la sécurité des systèmes dans le temps;
- le maintien de mécanismes de surveillance humaine effectifs, garantissant que les décisions appuyées par l'IA demeurent sous responsabilité humaine;
- des canaux de signalement et de recours accessibles pour les travailleuses et les travailleurs;
- les enjeux en matière de santé et de sécurité du travail aux mécanismes de gouvernance et de prévention existants.

## Phase 5

### DÉPLOIEMENT ET UTILISATION

#### Sensibilisation des travailleuses et des travailleurs

- Fournir des repères sur les principes de base de l'IA, ses usages concrets et ses finalités en milieu de travail.
- Sensibiliser les personnes aux limites des systèmes d'IA.
- Sensibiliser les personnes aux enjeux en santé et en sécurité du travail.
- Informer sur les obligations légales applicables.
- Clarifier les règles internes encadrant l'utilisation des outils d'IA.
- Rappeler l'importance du jugement humain et du contrôle dans les décisions appuyées par des systèmes d'IA.
- Adapter les actions de sensibilisation à l'évolution des usages et des technologies dans le temps.

#### Communication interne et culture d'innovation responsable

- Clarifier et diffuser les usages permis ou interdits de l'IA, ainsi que les conditions d'utilisation.
- S'assurer que l'information est accessible, compréhensible et adaptée à l'ensemble des travailleuses et des travailleurs.
- Porter attention aux usages informels ou non déclarés, notamment en lien avec des outils externes.
- Favoriser une culture organisationnelle ouverte à la discussion sur l'IA, qui inclut ses usages, ses bénéfices et ses limites.
- Encourager des espaces d'échange permettant la participation des différentes parties prenantes.
- Intégrer les enjeux liés aux conditions de travail, à la santé et à la sécurité du travail et aux effets sur les personnes dans les réflexions.
- Envisager l'innovation comme un processus évolutif, appelé à s'ajuster en fonction des pratiques et des expériences.

## Phase 6

### EXPLOITATION ET SUIVI

#### Suivi continu et adaptation des systèmes d'IA

- Assurer un suivi régulier des risques liés à l'IA, conformément aux principes de prévention prévus par la Loi sur la santé et la sécurité du travail.
- Identifier les nouveaux risques ou l'évolution des risques existants, notamment en matière de santé et de sécurité du travail, de charge de travail ou de risques psychosociaux.
- Mettre à jour les programmes de prévention, lorsque ceux-ci existent, afin d'y intégrer les risques liés à l'utilisation de l'IA.
- Ajuster les mesures de prévention lorsque les constats issus du suivi révèlent des effets non prévus ou des dérives.
- Consigner dans un document les constats et les ajustements apportés, afin de soutenir la prévention et le dialogue au sein des structures existantes.
- S'assurer que les mises au point maintiennent une supervision humaine adéquate et demeurent compatibles avec les réalités du travail.

## Phase 7

### MISE HORS SERVICE

#### Détermination des modalités de retrait, de désactivation ou de remplacement

- Définir et communiquer les modalités de retrait, de désactivation ou de remplacement d'un système d'IA au sein de l'organisation.
- Établir des critères clairs pouvant justifier la mise hors service d'un système, en cohérence avec les objectifs initiaux du projet d'IA.
- Évaluer les effets du retrait, de la désactivation ou du remplacement sur les travailleuses et les travailleurs.
- Prévoir les effets opérationnels de la mise hors service sur les activités et les processus.
- Prévoir une transition graduelle ou des mesures d'accompagnement pour les personnes concernées.
- Tenir compte des contraintes juridiques et contractuelles associées au retrait, à la désactivation ou au remplacement du système.

#### Gestion responsable des données associées aux systèmes en fin de vie

- Identifier les types de données concernés.
- Déterminer le sort des données associées au système.
- Fixer des durées de conservation appropriées, en fonction des finalités initiales et des obligations légales applicables.
- Mettre en œuvre des mesures de sécurité adaptées afin de prévenir les fuites de données ou les accès non autorisés.

#### Évaluation des effets de la mise hors service sur le travail et sur la santé et la sécurité du travail

- Évaluer les effets de la mise hors service sur l'organisation du travail, afin d'assurer le respect des conditions de travail prévues par la Loi sur les normes du travail.
- Identifier les effets sur la santé, la sécurité et le bien-être, y compris les risques psychosociaux, conformément aux obligations de protection prévues par la Loi sur la santé et la sécurité du travail.
- Mettre en place les ajustements nécessaires pour maintenir des conditions de travail sécuritaires et respectueuses des droits des travailleuses et des travailleurs.
- Prévoir des mesures d'accompagnement adaptées afin de soutenir les travailleuses et les travailleurs durant la transition.

