IFACI
Elevating Impact

LE CERCLE D'ÉTHIQUE DES AFFAIRES
ÉTHIQUE & CONFORMITÉ DES ENTREPRISES

INTELLIGENCE ARTIFICIELLE
ÉTHIQUE, RISQUES ET CONTRÔLE

DES OUTILS POUR SE PRÉPARER AU RIA

Noms des contributeurs : Zineb BOUSTIL, Edwige CENDRES, Cécile COGEZ, Arnaud DOUVILLE, Céline DECAEN, Arnaud LAGRANGE, Iohann LE FRAPPER, Pascal MAHIER, Benoît MERCIER, Anne-Violaine MONNIÉ, Stéphane POITEVIN, Stéphanie SCOUPPE, Inna TOURÉ.

Rédaction : Louis COLIN

Édition : Novembre 2024

Tandis que la numérisation des sociétés s'accélère, les progrès réalisés en matière d'intelligence artificielle fascinent et interrogent. Les risques éthiques liés au déploiement de systèmes d'intelligence artificielle semblent à la mesure des opportunités qu'ils sont susceptibles de créer. Dans ce contexte, l'Union Européenne a souhaité encadrer l'utilisation et la commercialisation de tels outils, d'abord grâce au Règlement Général sur la Protection des Données (RPGD), dès 2018, puis avec le Règlement sur l'Intelligence Artificielle (RIA) ou AI Act, qui entrera progressivement en vigueur entre 2025 et 2027.

Ce guide, fruit d'une collaboration entre les membres de l'Institut Français des Auditeurs et Contrôleurs Internes et du Cercle d'Éthique des Affaires, vise à faire dialoguer différentes expertises afin d'identifier les bonnes pratiques permettant de maîtriser les risques éthiques qui naissent du déploiement de systèmes d'IA[1] (SIA).

Il est composé de quatre outils à portée pratique :

- **Une cartographie des risques éthiques** liés à la conception, le déploiement, l'utilisation ou la commercialisation de SIA ;
- **Un formulaire de qualification des risques de pré-filtrage** à destination des équipes opérationnelles en charge de la conception, de l'utilisation ou de la commercialisation de SIA ;
- **Un questionnaire renforcé d'évaluation des risques éthiques** à destination des équipes en charge du contrôle de la conformité des SIA conçus, utilisés ou commercialisés avec les réglementations en vigueur et la politique éthique de leur entreprise ;
- **Une liste des contrôles** requis et recommandés afin d'établir un plan de contrôle interne dédié à ces enjeux.

Ce document pourra servir de base utile aux entreprises qui souhaiteraient anticiper l'entrée en vigueur définitive du RIA en 2027. Il a vocation à être mis à jour et enrichi des pratiques professionnelles qui naîtront grâce aux retours d'expérience sur les systèmes de management des risques liés au SIA déployés en entreprise.

I. CARTOGRAPHIE DES RISQUES

Cette partie a vocation à préciser les différents risques éthiques que peuvent engendrer le déploiement, la conception ou la commercialisation de SIA. Elle se veut pratique à défaut d'être exhaustive[2].

[1] Dans ce guide, la définition d'un système d'intelligence artificielle (SIA) est basée sur l'article 3 du RIA selon lequel : un SIA est un système basé sur une machine qui est conçu pour fonctionner avec différents niveaux d'autonomie et qui peut faire preuve d'adaptabilité après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer des environnements physiques ou virtuels.

[2] Le MIT a effectué une cartographie recensant 777 risques liés à l'IA, disponible ici : https://airisk.mit.edu/

L'éthique est une branche de la philosophie qui vise à s'interroger sur les principes régulateurs de l'action. Trois écoles d'éthique se distinguent particulièrement : l'éthique des vertus, l'éthique déontologique et l'utilitarisme, elles posent la question du bon, du juste ou de l'utile. Entendu de cette façon, l'éthique doit permettre d'envisager de façon large toutes les utilisations de SIA pouvant porter atteinte à l'intégrité et à la dignité des individus ou d'un groupe d'individus ainsi qu'aux droits et libertés fondamentaux qui en découlent.

Sont exclus les risques relatifs à la (cyber)sécurité des systèmes d'IA ainsi que les risques relatifs aux impacts environnementaux. Les enjeux de cybersécurité sont déjà couverts par d'autres réglementations en vigueur dont le respect échoit à des directions dédiées. Les impacts environnementaux des systèmes d'intelligence artificielle sont documentés et leur réduction est un impératif d'ordre légal et éthique. Néanmoins, ils ne feront pas ici l'objet de développement dans la mesure où les problématiques environnementales sont normalement couvertes, dans les entreprises, par des politiques dédiées.

L'absence ou la défaillance de la gouvernance dédiée au management des risques liés à la conception, l'utilisation, le déploiement de SIA sont entendues dans ce document comme des risques globaux de gouvernance englobant plusieurs risques décrits dans ce document. Plus largement, l'absence ou la défaillance de la gouvernance dédiée au management des risques liés à la conception, l'utilisation, le déploiement de SIA augmente la criticité de l'ensemble des risques décrits dans la grille ci-dessous.

En orange les risques relatifs à la conception, utilisation ou déploiement, de SIA dans un environnement non-spécifique

En vert les risques relatifs au déploiement de systèmes d'IA dans l'environnement de travail

En rose les risques relatifs à la commercialisation de systèmes d'IA

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Conditions de travail durant la phase de conception	Emploi de « travailleurs du clic » dont les conditions de travail ne respectent pas les conditions d'un travail digne : - Salaire décent - RPS	Déclaration OIT relative aux principes et droits fondamentaux au travail / Devoir de vigilance / CSRD	**Exemple :** Afin d'entraîner un SIA, des travailleurs sont rémunérés à la tâche, pour effectuer des actions à très faible valeur ajoutée telle que la labellisation de données.
Conditions de travail durant la phase de déploiement	Emploi de modérateurs dont les conditions de travail ne sont pas dignes : - Salaire décent - RPS	Déclaration OIT relative aux principes et droits fondamentaux au travail / Devoir de vigilance / CSRD	**Exemple :** Afin de modérer un espace numérique ou de qualifier certaines données, des travailleurs sont rémunérés pour visionner et labelliser des données au contenu violent.

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Conception non-inclusive	La conception d'un SIA est portée par une équipe dont la composition est susceptible d'entraîner des biais discriminatoires ou de ne pas refléter les attentes des utilisateurs.	Rapport Bias in algorithms - Artificial intelligence and discrimination de l'European Union Agency for Fundamental Rights	**Exemple :** La conception d'un modèle n'incluant pas une certaine représentativité sociologique (sexe, culture, catégorie socio-professionnel) ou d'intérêts (utilisateur, société civile) est susceptible d'entraîner des biais discriminatoires ou de ne pas être adapté à la pratique attendue par les utilisateurs.
Conception, utilisation ou déploiement d'outils ayant recours à des techniques subliminales	Conception, déploiement ou l'utilisation d'un SIA qui a recours à des techniques subliminales au-dessous du seuil de conscience d'une personne pour altérer substantiellement son comportement d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers.	Art. 5 a) AI Act	**Exemple :** Déploiement d'un outil de type réseau social interne reposant sur des techniques dites de « dark-patterns ».
Conception, utilisation ou déploiement d'outils à potentiel addictif	Le SIA repose sur une logique de fonctionnement favorisant les comportements addictifs des utilisateurs de l'outil.	Principes « Éthique de l'IA » de l'UNESCO – Principe « Proportionnalité et Innocuité »	**Exemple :** La création d'un réseau social reposant sur un modèle d'affaire reposant sur la publicité programmatique suppose de favoriser le temps d'utilisation des utilisateurs.
Conception, utilisation ou déploiement d'outils qui exploitent les éventuelles vulnérabilités dues à l'âge ou au handicap physique ou mental d'un groupe de personnes	Conception, déploiement ou l'utilisation d'un SIA qui exploite les éventuelles vulnérabilités dues à l'âge ou au handicap physique ou mental d'un groupe de personnes donné pour altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers.	Art. 5 b) AI Act	**Exemple :** Conception d'une plateforme de e-commerce comportant des « nudges » et des « dark-patterns » expressément conçus pour cibler des publics fragiles et visant à augmenter le panier moyen de dépenses.

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Conception, utilisation ou déploiement d'outils qui visent à instaurer un crédit social	Conception, déploiement ou l'utilisation, par les pouvoirs publics ou pour leur compte, de SIA destinés à évaluer ou à établir un classement de la fiabilité de personnes physiques au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues déduites ou prédites, la note sociale conduisant à l'une ou l'autre des situations suivantes, ou aux deux : i) le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes entiers de personnes physiques dans des contextes sociaux dissociés du contexte dans lequel les données ont été générées ou collectées à l'origine. ii) le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes entiers de personnes physiques, qui est injustifié ou disproportionné par rapport à leur comportement social ou à la gravité de celui-ci.	Art. 5 c)AI Act	**Exemple :** Conception et déploiement pour le compte d'un service public d'allocations d'indemnités chômage d'un SIA permettant d'agréger des données comportementales (données GPS, données tirées de réseaux sociaux personnels).
Conception, utilisation, déploiement de systèmes de surveillance et de profilage	Conception, déploiement ou utilisation de SIA visant à prédire le risque qu'une personne physique commette une infraction pénale Ou SIA ayant pour effet de créer ou développer des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciale depuis internet ou de la vidéosurveillance.	Art 5. d) e) g) AI act et article 6	

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Conception, utilisation, déploiement de systèmes de surveillance et de profilage	Ou Systèmes de catégorisation biométrique qui catégorisent individuellement les personnes physiques sur la base de leurs données biométriques afin d'arriver à des déductions ou des inférences concernant leur race, leurs opinions politiques, leur affiliation à une organisation syndicale, leurs convictions religieuses ou philosophiques, leur vie sexuelle ou leur orientation sexuel.		**Exemple :** Conception d'un système dit de reconnaissance facial permettant la détection des visages humains et l'identification des visages contenus dans une base de données regroupant les individus détenteur un casier judiciaire.
Conception, utilisation, déploiement de systèmes de prédiction des émotions	Conception, utilisation, déploiement de SIA pour inférer les émotions d'une personne physique sur le lieu de travail et dans les établissements d'enseignement.	Art 5. f) AI act et Art. 6	**Exemple :** Conception d'un système de prédiction des émotions pour déploiement à des fins de sécurité dans un environnement scolaire.
Utilisation de systèmes de surveillance à des fins répressives	Utilisation de systèmes d'identification biométrique à distance « en temps réel » dans des espaces accessibles au public à des fins répressives.	Art. 5 h) AI Act et art. 6	**Exemple :** Utilisation d'un système de reconnaissance faciale dans l'objectif d'identifier préventivement les individus aux comportements perturbateurs de façon à faire procéder à leur interpellation.
Conception de systèmes d'IA pouvant produire des décisions automatisées entraînant des effets juridiques	Conception de SIA dont l'utilisation peut mener à arrêter des décisions automatisées produisant des effets juridiques ou affectant de manière significative un individu donné.	Pas de base légale (extension article 22 RGPD)	**Exemple :** Conception d'un logiciel de tri de CV de 1er rang sans revue humaine.
Utilisation ou déploiement de systèmes d'IA produisant de façon automatique des effets juridiques sur les individus	Utilisation ou déploiement de SIA permettant d'arrêter des décisions automatisées produisant des effets juridiques ou affectant de manière significative un individu donné.	Art. 22 RGPD et arrêt Schufa	**Exemple :** Utilisation d'un logiciel de notation de la capacité d'emprunt bancaire sans revue humaine.

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Conception, utilisation, déploiement de systèmes destinés à être utilisés comme des composants de sécurité d'infra-structures critiques	Infrastructures critiques : SIA destinés à être utilisés comme composants de sécurité dans la gestion et l'exploitation d'infrastructures numériques critiques, dans le trafic routier ou dans la fourniture d'eau, de gaz, de chauffage ou d'électricité.	Article 6 AI Act, Annexe III.2	**Exemple :** Utilisation d'un système apprenant de fermeture des portes du métro dans un but d'optimisation du temps de trajet. Risque de fermeture prématurée ou de non-ouverture des portes.
Conception, utilisation, déploiement de systèmes destinés à être utilisés dans l'environnement scolaire ou de la formation	Systèmes visant à : Déterminer l'accès, l'admission ou l'affectation de personnes physiques à des établissements d'enseignement et de formation professionnelle Ou Évaluer les résultats de l'apprentissage Ou Évaluer le niveau d'éducation approprié qu'une personne recevra ou pourra atteindre Ou Surveiller et détecter les comportements interdits des étudiants lors des tests	Article 6 AI Act, Annexe III.3	**Exemple :** Conception et déploiement d'un SIA de notation automatique d'un oral.
Conception, utilisation, déploiement de systèmes pour gestion des travailleurs et accès à l'emploi	Systèmes pouvant être : Utilisés pour le recrutement ou la sélection de personnes physiques, notamment pour publier des offres d'emploi ciblées, pour analyser et filtrer les candidatures et pour évaluer les candidats Ou Utilisés pour prendre des décisions concernant les conditions des relations de travail, la promotion ou la résiliation des relations contractuelles liées au travail, pour attribuer des tâches sur la base du comportement individuel ou de traits ou caractéristiques personnels, ou pour surveiller et évaluer les performances et le comportement des personnes dans le cadre de ces relations.	Article 6 AI Act, Annexe III.4	**Exemple :** Conception et déploiement d'un SIA de tri automatisé des CV.

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Conception, utilisation, déploiement de systèmes permettant l'accès aux services essentiels	Systèmes pouvant être : Utilisés par les autorités publiques ou pour le compte de celles-ci afin d'évaluer l'éligibilité des personnes physiques aux prestations et services essentiels d'assistance publique, y compris les services de santé, ainsi que pour octroyer, réduire, supprimer ou réclamer ces prestations et services ; Ou Utilisés pour évaluer la solvabilité des personnes physiques ou établir leur score de crédit, à l'exception des SIA utilisés à des fins de détection de la fraude financière ; Ou Utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques dans le cas de l'assurance vie et de l'assurance maladie Ou Destinés à évaluer et à classer les appels d'urgence émanant de personnes physiques ou à être utilisés pour répartir les services de première intervention d'urgence, y compris la police, les pompiers et l'aide médicale, ou pour établir un ordre de priorité dans la répartition de ces services, ainsi que les systèmes de triage des patients dans le cadre des soins de santé d'urgence.	Article 6 AI Act, Annexe III.5	**Exemple :** Conception ou utilisation d'un SIA permettant dans la phase précontractuelle à un établissement de crédit d'évaluer la capacité d'emprunt d'un potentiel client et la possibilité d'y prétendre.
Conception, utilisation, déploiement de systèmes visant l'administration de la justice ou touchant au processus démocratique	Systèmes visant à : Être utilisés par une autorité judiciaire ou en son nom pour l'aider à rechercher et à interpréter les faits et le droit et à appliquer le droit à un ensemble concret de faits Ou Être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le vote de personnes physiques dans l'exercice de leur droit de vote lors d'élections ou de référendums.	Article 6 AI Act, Annexe III.8	**Exemple :** Conception et déploiement d'un SIA permettant à une juridiction de première instance de proposer un montant d'indemnité donnée en cas de procédure civile conformément à la jurisprudence applicable.

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Conception, utilisation ou déploiement de système d'IA opaques	SIA dont les logiques de fonctionnement sont opaques et/ou non-intelligibles pour l'utilisateur.	Principes OCDE pour l'IA – Transparence et Explicabilité	**Exemple :** Utilisation d'un système de prédiction des maladies rares chez un patient qui ne permet pas au professionnel de santé utilisateur de connaître les variables ayant permis le diagnostic et/ou de comprendre le lien fait entre les variables constatées et la probabilité de développer une maladie rare par le patient.
Conception de système d'IA ayant un impact sur l'environnement de travail	Voir risques environnement de travail.	Convention Philadelphie 1944, grille d'analyse du LaborIA	Voir risques environnement de travail.
Atteinte à la confidentialité des données utilisées	Des données protégées ou confidentielles sont traitées par le SIA sans considération pour leur qualité particulière.	RGPD	**Exemple :** Un logiciel type ChatGPT interne à une entreprise dévoile à tous ceux qui y ont accès le niveau de rémunération de l'ensemble des salariés de l'entreprise.
Atteinte au sentiment reconnaissance d'un collaborateur	Remise en cause de la capacité de l'individu, de ses pratiques, de ses efforts, de sa contribution au travail de l'équipe ou de l'entreprise.	Convention Philadelphie 1944, grille d'analyse du LaborIA	**Exemple :** L'utilisation d'un logiciel type ChatGPT entraîne une confusion entre le travail humain et le travail de la machine et est à même de perturber la gratification reçue par le collaborateur pour sa production et le sentiment d'effort du collaborateur lui-même.

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Atteinte aux relations humaines	Le déploiement d'un SIA induit une dégradation des relations interpersonnelles dans l'environnement de travail.	Convention Philadelphie 1944, grille d'analyse du LaborIA	**Exemple :** Le déploiement d'un SIA de tri et de réponse automatique aux mails de complexité basse ou moyenne entraîne un isolement des collaborateurs entre eux et/ou un isolement de l'équipe utilisatrice vis-à-vis des autres services. Il peut, de façon similaire, remplacer des temps de brainstorming collectifs nécessaires à l'entente, la solidarité et la compréhension entre collaborateurs.
Contrôle du travail / surveillance	Le déploiement d'un SIA renforce le sentiment de contrôle du travail ou de surveillance par l'utilisateur susceptible d'entraîner des RPS.	Convention Philadelphie 1944, grille d'analyse du LaborIA	**Exemple :** Utilisation d'un logiciel d'aide à la décision dans des entrepôts de stockage. Le logiciel effectue des recommandations d'ordre impérative à l'agent qui n'a d'autres choix que de les respecter. L'action de l'agent utilisateur peut être également évaluée (productivité horaire) et monitorée en temps réel.
Atteinte à l'autonomie et risque d'aliénation	Le déploiement d'un SIA réduit l'espace de jugement / d'action et induit une baisse du libre arbitre.	Convention Philadelphie 1944, grille d'analyse du LaborIA	**Exemple :** Une équipe de maintenance utilise un système de prédiction des pannes qui induit un protocole très dirigé basé sur une architecture de choix limités.
Atteinte au savoir-faire	Le déploiement d'un SIA entraîne la surpression de certaines tâches, notamment à peu de valeur ajoutée, qui produisent chez l'individu un sentiment de perte contrôle et de confiance.	Convention Philadelphie 1944, grille d'analyse du LaborIA	**Exemple :** Un logiciel de prise automatique de note remplace la prise de note et la rédaction de compte-rendu de réunion par le collaborateur. Tâche peu complexe, elle permet néanmoins au collaborateur de mieux comprendre son environnement de travail, d'ordonner sa pensée et de ressentir de la confiance vis à vis de ses propres compétences.

Type de risque	Description du risque	Base légale / éthique	Scénarios de risque
Responsabilité en cas de faute dans l'environnement de travail	Le déploiement d'un SIA brouille la chaîne de responsabilité en cas de dysfonctionnement, erreur ou négligence grave dans l'environnement de travail.	Convention Philadelphie 1944, grille d'analyse du LaborIA	**Exemple :** Un SIA entraîne des conséquences négatives sans qu'il ne soit aisé de comprendre en première instance si la faute découle d'une mauvaise utilisation de l'outil par l'utilisateur, d'une erreur de l'outil, d'un manque de supervision de l'outil et des équipes utilisatrices.
Utilisation négligente d'un système d'IA	L'utilisateur n'a pas été formé à l'utilisation du SIA, ne dispose pas ou n'exerce pas un recul critique face aux résultats proposés par le SIA ou l'utilise de façon négligente.		**Exemple :** Utilisation d'un logiciel type ChatGPT pour résoudre des problématiques d'ordre technique dans l'industrie. Mise en œuvre sans vérification de la proposition effectuée par le logiciel entraînant une panne.
Détournement de l'usage prévu d'un système d'IA	Le client détourne l'usage du SIA commercialisé dans un objectif non prévu par le concepteur et contraire à sa politique d'éthique.	Politique d'éthique interne / CSRD	**Exemple :** Commercialisation d'un outil d'analyse marketing des réseaux sociaux paramétré par un client public comme outil de profilage politique.
Utilisation d'un système d'IA comme composant d'une technologie risquée	Le client utilise le SIA comme le composant d'une technologie contraire à la politique d'éthique du vendeur.	Art. 6 AI ACT	**Exemple :** Commercialisation d'un outil de reconnaissance d'image utilisé par le client dans un système d'armement autonome.
Commercialisation d'un système d'IA visé par l'article 5 de l'AI Act	Commercialisation d'un SIA dont la fonctionnalité est expressément interdite par l'AI Act.	Art. 5 AI Act	**Exemple :** Commercialisation d'un outil de reconnaissance faciale permettant de déduire les émotions des salariés sur leur lieu de travail.

II. FORMULAIRE DE QUALIFICATION DU RISQUE DE PRÉFILTRAGE

Ce formulaire a vocation à être transmis aux équipes d'opérationnels ayant la charge de déployer, utiliser ou commercialiser un SIA pour leur permettre de procéder à une analyse de premier niveau du risque éthique porté par le système.

A | Contexte

1) Description de la finalité du projet et de ces cas d'usage à court et moyen-terme :

.....

.....

2) Calendrier de mise en service du système : .....

3) Objectifs pour l'utilisateur : .....

.....

Enjeux pour l'entreprise, et mesures de suivi : .....

.....

Alternatives éventuelles envisagées au projet : .....

.....

B | Système

1) Type de système :

☐ IA générative ☐ Machine-learning ☐ Apprentissage dirigé
☐ Règles de calcul codées par des personnes sans apprentissage

2) Maîtrise du système :

a. S'agit-il d'un projet en : Développement interne ☐ Développement externe ☐

b. Quels sont les éléments de maîtrise du système ?

.....

3) Le système traite-t-il des données de l'entreprise : ☐ Oui ☐ Non

Si oui, pour quelles finalités :

☐ Entraînement ☐ Fonctionnement et exploitation ☐ Après traitement par l'IA ☐ Autres

4) Liste des données manipulées lors de la phase d'apprentissage et, si connue, source de ces données :

.....

.....

5) Le système traite-t-il des données personnelles ? ☐ Oui ☐ Non

a. Si oui, pour quelles finalités :

☐ Entraînement ☐ Fonctionnement et exploitation ☐ Après traitement par l'IA ☐ Autres

a) Si oui, comment a été effectué l'information et le recueil de consentement des personnes visées ? .....

.....

2) Quel est le degré d'explicabilité de l'algorithme et de ses logiques de fonctionnement ? :

☐ Facilement explicable au public ☐ Explicable mais complexe ☐ Non explicable au public

C | Enjeux éthiques

1) Quels sont les impacts du système sur :

a. L'organisation, la gouvernance et les process de l'entreprise :

.....

b. Les personnes salariées :

Renseignez notamment le type de population exposée, nombre et pourcentage de personnes directement ou indirectement affectées par le traitement et la nature de l'impact, l'impact financier, sur le bien-être et qualité de vie au travail, sur les compétences, sur la qualité des relations.

.....

c. Les personnes externes :

Renseignez le type de population exposée, nombre de personnes directement ou indirectement affectés par le traitement, l'impact financier ou moral faible ou significatif.

d. La réputation de l'entreprise :

.....

e. L'environnement :

Renseignez notamment la consommation énergétique.

.....

2) Le système d'IA pourrait-il entraîner un risque de discrimination ? Existe-t-il un cas d'usage de discrimination connu pour un système de ce type ?

.....

3) Quel est le degré d'automatisation permis par le système ?

☐ Faible, participation à la décision

☐ Moyen, participation avec recommandation et conseil avant décision

☐ Fort, décision sans intervention humaine

4) Quel est le degré d'autonomie du système l'IA ?

☐ **Gérée par l'humain :** prise de décision humaine à chaque étape

☐ **Autonomie relative :** l'IA prend des décisions autonomes sans conséquences directes dans le monde réel

☐ **Autonomie partielle :** l'IA peut prendre des décisions ou actions autonomes avec conséquences directes dans le monde réel et existence d'une revue ou d'une intervention humaine

☐ **Autonomie complète :** le système reçoit les objectifs à atteindre par l'humain et les traduit en tâches et décisions sans interaction humaine

5) Seriez-vous à l'aise avec ce projet dans tous les contextes politiques ?

.....

6) Existe-t-il des opportunités (impacts positifs) en relation avec les thématiques identifiées au point 1 ?

.....

D | Mesures de limitation des risques

1) Quelles sont les actions mises en place pour identifier et prévenir les potentiels biais, hallucinations ou détournements d'usage ?

.....

2) Quelle gouvernance envisagée pour suivre le projet dans sa durée ?

.....

3) Quels sont les outils et indicateurs de suivi envisagés ?

.....

4) Quel accompagnement est prévu pour les collaborateurs affectés par le déploiement du système ?

.....

5) Existe-t-il des clauses contractuelles pour couvrir les risques identifiées ?

.....

III. QUESTIONNAIRE RENFORCÉ D'ÉVALUATION DES RISQUES ÉTHIQUES

Ce questionnaire a vocation à être utilisé par les experts juridiques, éthiques, de l'audit et du contrôle interne pour évaluer le risque juridique et éthique porté par un projet d'IA. Ils n'ont pas vocation à être transmis aux opérationnels.

QUESTIONNAIRE 1 : CONCEPTION OU COMMERCIALISATION D'UN SIA

EXIGENCES LÉGALES

1) **La conception et/ou la mise en œuvre du projet / système d'IA vise-t-elle, induit-elle ou repose-t-elle sur : (Art. 5 du RIA)**
   a. Exploitation de techniques subliminales ☐ Oui ☐ Non
   b. Exploitation des vulnérabilités chez l'utilisateur lié à l'âge ou au handicap ☐ Oui ☐ Non
   c. Instauration d'un crédit social ☐ Oui ☐ Non
   d. Prédiction du risque pénal d'une personne physique ☐ Oui ☐ Non
   e. Reconnaissance faciale par moissonnage d'images faciales provenant d'Internet ou de la vidéosurveillance ☐ Oui ☐ Non
   f. Prédiction des émotions d'une personne physique sur le lieu de travail ou les établissements d'enseignement ☐ Oui ☐ Non
   g. Catégorisation des personnes physiques sur la base de leur données biométriques pour prédire la race, les opinions politiques, les affiliations à une organisation syndicale, les convictions religieuses ou philosophiques, leur vie ou leur orientation sexuelle. ☐ Oui ☐ Non

   ▶ **Si oui à l'une de ces options, non-conformité.**

2) **La conception et/ou la mise en œuvre du projet / système d'IA vise-t-elle à utiliser des systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives ? (Art.5 du RIA)** ☐ Oui ☐ Non

   ▶ **Si oui, s'assurer que c'est dans l'objectif de :**

   a. Recherche ciblée de victimes d'enlèvement, de traite ou d'exploitation sexuelle ou de personnes disparues ;
   b. Prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou menace réelle, actuelle ou prévisible d'attaques terroristes ;
   c. Localisation ou identification d'une personne soupçonnée d'avoir commis une infraction pénale.

   ▶ **Si non, non conformité.**

Si votre entreprise est fournisseuse, qu'elle conçoit et/ou commercialise le système d'IA

Éléments à contrôler :

- Existence d'un système de gestion des risques couvrant l'ensemble du cycle de vie de l'outil ☐ Oui ☐ Non
- Pertinence du système de gestion des risques eu égard à :
- Identification des risques connus et raisonnablement prévisible en matière de santé, sécurité ou droits fondamentaux en cas d'utilisation conforme de l'outil
- Estimation et évaluation des risques en cas d'utilisation conforme et dans des conditions de mauvaises utilisations raisonnablement prévisibles
- Adoption de mesures appropriées et ciblées de gestion de risque
- Existence de mesures de contrôle de la qualité des jeux de données d'entraînement, de validation de teste (art. 10 du RIA) ☐ Oui ☐ Non
- Existence d'une documentation technique conforme à l'annexe IV du RIA (Art. 11 du RIA) ☐ Oui ☐ Non
- Existence de fonctionnalités de journalisation permettant l'enregistrement des événements suggérant l'existence de risques éthiques (Art. 12 du RIA) ☐ Oui ☐ Non
- Existence d'une notice d'utilisation dans un format numérique approprié ou autre, contenant des informations concises, complètes, exactes et claires, qui soient pertinentes, accessibles et compréhensibles pour les déployeurs (Art. 13 du RIA) ☐ Oui ☐ Non
- Existence de mesures de contrôle proportionnées aux risques, au niveau d'autonomie et au contexte d'utilisation du système d'IA à haut risque intégrés au SIA ou aménageables par le déployeur (Art. 14 du RIA) ☐ Oui ☐ Non

Si votre entreprise déploie un système d'IA qu'elle n'a pas conçu

Éléments à contrôler :

- Existence de mesures techniques et organisationnelles appropriées afin de garantir une utilisation du SIA conforme aux notices d'utilisation accompagnant les systèmes (Art. 26 RIA) ☐ Oui ☐ Non
- Existence d'une gouvernance permettant un contrôle humain par des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires ainsi que du soutien nécessaire. (Art. 26 RIA) ☐ Oui ☐ Non

3) **La conception et/ou la mise en œuvre du projet / système d'IA donné est-elle respectueuse de conditions de travail dignes ? (CS3D)** ☐ Oui ☐ Non

Si votre entreprise est fournisseuse, qu'elle conçoit et/ou commercialise le système d'IA

Éléments à contrôler :

- Respect par le prestataire et les sous-traitants impliqués dans le projet donné des principes de la déclaration OIT, notamment salaire décent et atténuation des risques psychosociaux. ☐ Oui ☐ Non

4) **Le projet / système d'IA peut-il avoir produit des effets juridiques ou affecter de manière significative un individu ? (art.22 RGPD)** ☐ Oui ☐ Non

Si oui :

A. **Est-il possible pour l'individu affecté par une décision/recommandation du système d'IA de contester ou de demander l'intervention d'un être humain concernant la décision prise ?** ☐ Oui ☐ Non

Éléments à contrôler : Existe-t-il ?

- Un dispositif de contestation ☐ Oui ☐ Non
- Une revue humaine de la décision ☐ Oui ☐ Non
- Une recommandation prise par l'IA par un opérateur humain ? ☐ Oui ☐ Non

Si non, potentielle non-conformité (Arrêt Schufa).

B. **La conception et/ou la mise en œuvre du projet / système d'IA est-elle susceptible d'entraîner des biais discriminatoires ?** ☐ Oui ☐ Non

Le cas échéant, lesquels ?

.....

.....

Éléments à contrôler :

- Représentativité des équipes de développements du système.
- Représentativité des données d'entraînement des modèles.
- Impartialité des logiques de fonctionnement et des variables clefs
- Une recommandation prise par l'IA par un opérateur humain ? ☐ Oui ☐ Non

C. Le projet / système d'IA vise-t-il à introduire dans un environnement scolaire ou de formation des dispositifs visant à :

a. Déterminer l'accès, l'admission ou l'affectation de personnes physiques à des établissements d'enseignement et de formation professionnelle ☐ Oui ☐ Non

b. Évaluer les résultats de l'apprentissage ☐ Oui ☐ Non

c. Évaluer le niveau d'éducation approprié qu'une personne recevra ou pourra atteindre ☐ Oui ☐ Non

d. Surveiller et détecter les comportements interdits des étudiants lors des tests ☐ Oui ☐ Non

▶ Si oui :

Éléments à contrôler : Idem point 2.

D. Le projet / système d'IA permet-il de faciliter la gestion des travailleurs et l'accès à l'emploi ?

- Recrutement ☐ Oui ☐ Non
- Promotion ☐ Oui ☐ Non
- Attribution de tâches ☐ Oui ☐ Non
- Licenciement ☐ Oui ☐ Non

▶ Si oui :

Éléments à contrôler : Idem point 2.

E. Le projet / système d'IA vise-t-il ou peut-il conduire à conditionner l'accès à des services essentiels

- Services publics ☐ Oui ☐ Non
- Prestations et aides ☐ Oui ☐ Non
- Solvabilité ☐ Oui ☐ Non
- Assurance ☐ Oui ☐ Non
- Police ☐ Oui ☐ Non
- Aide médicale et santé ☐ Oui ☐ Non

▶ Si oui :

Éléments à contrôler : Idem point 2.

F. Le projet / système d'IA vise-t-il ou peut-il conduire à faciliter l'administration de processus judiciaires ou démocratiques ? ☐ Oui ☐ Non

▶ Si oui :

Éléments à contrôler : Idem point 2.

5) **La mise en œuvre / l'utilisation du projet / système d'IA fait-elle courir le risque d'atteinte à la confidentialité des données ?** ☐ Oui ☐ Non

Éléments à contrôler :

- Le fonctionnement du système repose-t-il sur des logiques de maximisation des données récoltées ? ☐ Oui ☐ Non
- Existence de contrôles cybersécurités ☐ Oui ☐ Non

RECOMMANDATIONS ÉTHIQUES

6) **Est-ce que les décisions arrêtées par le système d'IA sont susceptibles d'atteindre à la charte éthique de l'entreprise ?** ☐ Oui ☐ Non

7) **Les logiques de fonctionnement du projet / système d'IA sont-elles transparentes, intelligibles et facilement accessibles à l'utilisateur ?** ☐ Oui ☐ Non

Éléments à contrôler :

- Explicabilité du modèle : l'utilisateur a-t-il facilement accès à un support aisément compréhensible des logiques de fonctionnement du modèle d'IA, (notamment : les données utilisées, les règles de fonctionnement de l'algorithme, les relations entre données d'entrée et de sortie, les cas d'usages conformes de l'algorithme, les limites et les risques d'erreurs ou d'« hallucination » du modèle).

8) **L'utilisation du projet / système d'IA est-elle susceptible d'entraîner chez ses utilisateurs des effets d'addiction ?** ☐ Oui ☐ Non

Éléments à contrôler :

- Le fonctionnement du système repose-t-il sur des logiques de maximisation du temps d'utilisation ? ☐ Oui ☐ Non
- Existe-t-il des alertes et des dispositifs de limitation du temps d'utilisation intégré au système ? ☐ Oui ☐ Non
- Existe-t-il des alertes et des dispositifs de limitation relatifs aux transactions financières effectuées ou facilitées par le système ? ☐ Oui ☐ Non

9) La chaîne de responsabilité relative à l'utilisation, le déploiement ou la mise en œuvre du projet/système d'IA est-elle précisément définie et connue des auteurs qui en ont la charge ?

☐ Oui ☐ Non

Éléments à contrôler :

- Existence d'une matrice de responsabilité pour les utilisateurs du système d'IA.
- Existence d'une gouvernance encadrant le déploiement du système d'IA.

10) Existe-t-il un risque d'utilisation détournée du système d'IA par le client prévisible et portant atteinte aux droits et libertés fondamentales ? ☐ Oui ☐ Non

▶ Si oui :

Éléments à contrôler :

- Estimation du risque prévisible de détournement d'usage par le client (réputation, risque et situation politique)
- Existence d'un système de gestion des risques couvrant l'ensemble du cycle de vie de l'outil
- Examen et mise à jour périodique du système de gestion des risques
- Pertinence du système de gestion des risques eu égard à :
  - Identification des risques connus et raisonnablement prévisible en matière de santé, sécurité ou droits fondamentaux en cas d'utilisation conforme de l'outil
  - Estimation et évaluation des risques en cas d'utilisation conforme et dans des conditions de mauvaises utilisations raisonnablement prévisibles
  - Adoption de mesures appropriées et ciblées de gestion de risque

Questionnaire 2 : Déploiement d'un SIA sur le lieu de travail

EXIGENCES LÉGALES

1) **Le déploiement du système d'IA vise-t-il à la prédiction des émotions d'une personne physique sur le lieu de travail ou les établissements d'enseignement** ☐ Oui ☐ Non

   ▶ **Si oui, non-conformité.**

2) **Le système d'IA est-il considéré à haut risque au sens du RIA ?** ☐ Oui ☐ Non

   Si oui, obligation d'information aux instances représentatives du personnel du déploiement du SIA.

3) **Le système d'IA peut-il avoir produit des effets juridiques ou affecter de manière significative un individu ?** ☐ Oui ☐ Non

   ▶ **Si oui :**

   A. **Est-il possible pour l'individu affecté par une décision/recommandation du système d'IA de contester ou de demander l'intervention d'un être humain concernant la décision prise ?**

   Éléments à contrôler : Existe-t-il ?

   - Un dispositif de contestation ☐ Oui ☐ Non
   - Une revue humaine de la décision ☐ Oui ☐ Non
   - Une recommandation prise par l'IA par un opérateur humain ☐ Oui ☐ Non

   ▶ **Si non, potentielle non-conformité.**

   B. **La conception et/ou la mise en œuvre du projet / système d'IA est-elle susceptible d'entraîner des biais discriminatoires ? Le cas échéant, lesquels ?**

   Éléments à contrôler :

   - Représentativité des équipes de développements du système.
   - Représentativité des données d'entraînement des modèles.
   - Impartialité des logiques de fonctionnement et des variables clefs.

4) **Le déploiement du système d'IA permet-il de faciliter la gestion des travailleurs et l'accès à l'emploi**

   - Recrutement ☐ Oui ☐ Non
   - Promotion ☐ Oui ☐ Non
   - Attribution de tâches ☐ Oui ☐ Non
   - Licenciement ☐ Oui ☐ Non

Si oui :

Éléments à contrôler (art. 9) :

- Existence d'un système de gestion des risques couvrant l'ensemble du cycle de vie de l'outil
- Examen et mise à jour périodique du système de gestion des risques
- Pertinence du système de gestion des risques eu égard à :
- Identification des risques connus et raisonnablement prévisibles en matière de santé, sécurité ou droits fondamentaux en cas d'utilisation conforme de l'outil
- Estimation et évaluation des risques en cas d'utilisation conforme et dans des conditions de mauvaises utilisations raisonnablement prévisibles
- Adoption de mesures appropriées et ciblées de gestion de risque

RECOMMANDATIONS ÉTHIQUES

5) **Les logiques de fonctionnement du projet / système d'IA sont-elles intelligibles et transparentes et facilement accessibles à l'utilisateur ?** ☐ Oui ☐ Non

Éléments à contrôler :

- Explicabilité du modèle : l'utilisateur a-t-il facilement accès à un support aisément compréhensible des logiques de fonctionnement du modèle d'IA, (notamment : les données utilisées, les règles de fonctionnement de l'algorithme, les relations entre données d'entrée et de sortie, les cas d'usages conformes de l'algorithme, les limites et les risques d'erreurs ou d'« hallucination » du modèle).

6) **Le déploiement du système d'IA est-il susceptible :**

a. d'atteinte au sentiment de reconnaissance d'un salarié ☐ Oui ☐ Non

b. d'atteinte à la qualité des relations humaines des salariés utilisateurs dans leur environnement de travail ☐ Oui ☐ Non

c. d'atteinte à l'autonomie du salarié ☐ Oui ☐ Non

d. d'atteinte au savoir-faire du salarié ☐ Oui ☐ Non

e. de fausser le partage de responsabilité en cas de faute ☐ Oui ☐ Non

Éléments à contrôler :

- Estimation préalable au déploiement du système d'IA du nombre de postes et du volume de tâches par postes (en pourcentage et en volume horaire) exposés à la numérisation.

- Tableau de répartition des tâches effectuées par l'opérateur, sans, avec et en collaboration avec l'outil et de la répartition de responsabilité pour chaque tâche.
- Existence d'un plan de communication, acculturation, à destination de l'ensemble des salariés.
- Existence d'un plan de formation à destination des salariés utilisateurs et encadrants.
- Existence d'un dispositif de prévention des RPS.
- Mise en place d'un temps d'échange dédié pour les salariés utilisateurs.
- Existence d'un plan d'évaluation régulier du système d'IA (productivité des utilisateurs, satisfaction des utilisateurs, difficultés rencontrées) et d'amélioration continue de l'intégration de l'outil à l'environnement de travail.
- Existence d'un plan de contrôle interne dédié aux systèmes IA.
- Ouverture des lignes d'alerte interne aux sujets liés au déploiement de systèmes d'IA dans l'environnement de travail.

7) Le déploiement du système d'IA est-il susceptible de renforcer le sentiment de contrôle / surveillance travail ? ☐ Oui ☐ Non

Éléments à contrôler :

- Idem point 3.
- Vigilance particulière en cas de monitoring en temps-réel de la productivité d'une personne physique.

III. ÉLÉMENTS DE CONTRÔLE INTERNE

Sur la base des risques identifiés et des scénarios correspondants, il est recommandé de mettre en place un plan de contrôle interne permettant de vérifier l'existence d'une gouvernance dédiée au management des risques éthiques liées à l'utilisation, le déploiement ou la commercialisation de SIA, la conformité de ces systèmes à la réglementation en vigueur, la couverture contractuelle en cas de commercialisation, et le respect et la prévention des risques psychosociaux en cas de déploiement au sein de l'entreprise.

Le tableau ci-dessous énonce une liste de 34 contrôles, dont 9 ont été identifiés comme prioritairement requis par le groupe de travail.

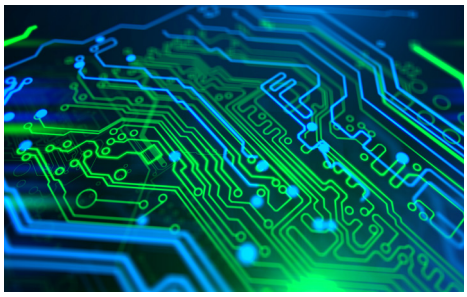
	Risques	Objectifs du contrôle	Contrôles	Priorité
1. GOUVERNANCE	L'absence d'un système de management des risques lié à l'IA peut entraîner des risques financiers, juridiques et réputationnels forts dès lors qu'elle révèle une non-conformité au RIA et une négligence aux conséquences potentiellement graves sur les individus et les libertés fondamentales des utilisateurs internes ou externes.	1.1. Un système de management des risques de l'IA, soutenu par le top management, permet l'identification, le suivi et la remédiation des risques causés par l'utilisation, le déploiement ou la commercialisation de traitement algorithmique.	1.1.1 S'assurer qu'il existe une Charte aisément accessible par l'ensemble des collaborateurs de l'entreprise et conforme à l'AI Act et au RGPD décrivant les principes auxquels est attachée l'entreprise dans l'utilisation, le déploiement ou la commercialisation de SIA.	Requis
			1.1.2 S'assurer qu'il existe une gouvernance en charge du soutien de la politique groupe définie et des mesures organisationnelles permettant son respect.	Requis
			1.1.3 S'assurer qu'il existe un responsable opérationnel en charge de la supervision et du respect de la politique groupe définie.	Requis
			1.1.4 S'assurer qu'il existe une matrice de responsabilité déterminant précisément les rôles et responsabilités techniques et opérationnelles afin de garantir une gestion des SIA conforme à la politique groupe définie.	Recommandé
			1.1.5 S'assurer que la politique groupe définie est soutenue par des procédures opérationnelles, des orientations ou des manuels pour guider le personnel opérationnel dans l'identification, le suivi et la remédiation des risques causés par l'utilisation, le déploiement ou la commercialisation de SIA.	Recommandé
			1.1.6 S'assurer que le top management soutient la politique groupe définie.	Bonne pratique
		1.2. Une analyse des impacts éthiques conforme à l'AI Act est menée pour chaque projet d'IA.	1.2.1 Chaque SIA déployé, utilisé ou commercialisé a fait l'objet d'une évaluation d'impact éthique de 1er niveau, conforme à l'AI Act.	Requis
			1.2.2 Les SIA relevant de la catégorie à « haut risque » en vertu de l'AI Act font l'objet d'une analyse d'impact couvrant l'entièreté du cycle de vie, régulièrement mise à jour.	Requis
			1.2.3 Chaque SIA dont l'analyse d'impact éthique a permis d'identifier des risques éthiques significatifs fait l'objet de mesures de remédiation suivi dans le temps.	Recommandé
			1.2.4 Il existe un registre des SIA utilisés, déployés et commercialisés par le Groupe, à compter d'une date définie.	Recommandé

	Risques	Objectifs du contrôle	Contrôles	Priorité
1. GOUVERNANCE	L'absence de procédure de traitement des contestations peut entraîner des risques juridiques et réputationnels important dans la mesure où ils peuvent révéler une violation des dispositions du RGPD et du RIA. Cette procédure doit permettre aux utilisateurs de ne pas être victimes de décision automatisée ayant des effets juridique ou les affectant significativement sur leur existence.	1.3 Il existe une procédure de traitement des demandes ou contestations relatives aux droits et libertés individuelles en matière de traitement algorithmique.	1.3.1 Il existe une procédure, diffusée largement à l'ensemble des utilisateurs visés par le système algorithmique déployé, leur permettant d'effectuer des demandes relatives au respect des droits et libertés individuelles en matière de traitement algorithmique.	Requis
			1.3.2 La procédure de traitement des demandes est placée sous la responsabilité d'une équipe dont les compétences transverses permettent l'évaluation de la demande et, le cas échéant, son bon traitement.	Bonne pratique
			1.3.3 L'effectivité du dispositif est contrôlée (Exemple : Mesure du temps de réponse moyen à une contestation).	Bonne pratique
2. SYSTÈME	L'opacité des SIA peut mener à des effets « boîtes noires » qui empêchent d'analyser la fiabilité et l'équité des SIA et de contrôler la pertinence des recommandations ou solutions proposées par le SIA. Risque de discrimination, de manque de fiabilité, de non-conformité.	2.1. Des mesures sont adoptées pour favoriser la transparence des systèmes algorithmiques.	2.1.1 Il existe une documentation pour les traitements algorithmiques à « haut risque » présentant de façon claire et intelligible et dans un langage courant les logiques de fonctionnement des traitements algorithmes utilisés et les variables qui influencent significativement leur résultat.	Requis
			2.1.2 Les conditions d'utilisation de chaque traitement algorithmique utilisé, déployé et commercialisé sont aisément accessibles par les utilisateurs dans leur langue maternelle.	Bonne pratique
			2.1.3 Si le traitement algorithmique utilise des données personnelles des utilisateurs, s'assurer de la bonne information de l'utilisateur de la finalité pour laquelle celles-ci sont utilisées.	Cf. Process RGPD
		2.2 Les systèmes algorithmiques sont régulièrement monitorés pour assurer leur fiabilité statistique et l'absence de biais discriminatoires.	2.2.1 S'assurer qu'il existe une documentation présentant le détail du processus de labellisation des données pour les systèmes à haut risque.	Bonne pratique
			2.2.2 Les systèmes algorithmiques susceptibles de présenter des biais discriminatoires sont régulièrement vérifiés pour évaluer leur fiabilité statistique et l'absence de biais discriminatoire.	Bonne pratique
			2.2.3 En cas de manquements relevés par les rapports de vérification sur la fiabilité statistique des systèmes algorithmiques, s'assurer que des mesures de remédiation ont été arrêtés et sont monitorées.	Bonne pratique

	Risques	Objectifs du contrôle	Contrôles	Priorité
2. SYSTÈME	Cette procédure doit permettre de se conformer aux exigences de l'article 22 du RGPD et de l'arrêt Schufa de la CJUE qui imposent une revue humaine pour toute décision automatisée produisant des effets juridiques ou affectant significativement un individu.	2.3 Les recommandations ou décisions arrêtées par les systèmes algorithmiques sont soumises à une revue humaine proportionnelle au niveau de risque identifié par l'analyse d'impact éthique.	2.3.1 Sur la base de l'analyse d'impact éthique, s'assurer que pour chaque SIA, sont définis les niveaux et les cas nécessaires ou possibles de revue humaine.	Recommandé
			2.3.2 S'assurer que chaque décision algorithmique faisant l'objet d'une revue humaine est enregistrée et correctement documentée.	Bonne pratique
			2.3.3 S'assurer que les personnes ou l'équipe effectuant la revue humaine dispose des compétences, de la formation, des ressources, et du temps nécessaire pour agir de façon appropriée.	Bonne pratique
3. CONTRAT ET TIERS	L'absence de due diligence et/ou de vigilance contractuelle peut entraîner des risques financiers, juridiques et réputationnels forts dès lors qu'elle révèle une non-conformité au RIA et une négligence aux conséquences potentiellement graves sur les individus et les libertés fondamentales des utilisateurs internes ou externes.	3.1 Les systèmes algorithmiques achetés auprès de fournisseurs respectent le réglementation et la politique d'éthique en vigueur dans le Groupe.	3.1.1 S'assurer pour chaque système algorithmique considéré à haut risque en vertu de l'AI Act que le fournisseur a rempli les obligations de conformité prévu par l'article 43 de l'AI Act.	Requis
			3.1.2 S'assurer que le processus de sélection du système algorithmique incluait une évaluation de la qualité du système de gestions des risques éthiques par le fournisseur.	Bonne pratique
			3.1.3 S'assurer que chaque contrat liant le Groupe à un fournisseur de système algorithmique contient : - Des dispositions relatives aux respects des droits humains (exemple : droit à un environnement de travail respectueux de la dignité humaine) ; - Des indicateurs de suivi de la performance précis et cohérents avec ceux mis en avant dans l'analyse d'impact éthique et justifiant le déploiement de l'outil ; - Un calendrier de revue périodique de la conformité du système à sa documentation technique.	Bonne pratique
		3.2 Le Groupe commercialise des systèmes algorithmiques à des clients qui en feront un usage conforme aux règles d'utilisation définies par le Groupe.	3.2.1 S'assurer pour chaque système algorithmique considéré à haut risque en vertu de l'AI Act, que le Groupe a rempli les obligations de conformité prévu par l'article 43 de l'AI Act.	Requis
			3.2.2 S'assurer pour chaque commercialisation de système algorithmique à risque significatif au regard de l'évaluation d'impact mené, qu'une évaluation éthique du client est menée, notamment au regard des risques portés par celui-ci eu égard aux libertés individuelles et du respect de l'état de droit.	Bonne pratique
			3.2.3 S'assurer que chaque contrat liant la Groupe à un client de système algorithmique contient : - Des dispositions relatives aux respects des droits humains (exemple :...) ; - Des indicateurs de suivi de la performance permettant d'évaluer la performance de l'outil de façon régulière ; - Un calendrier de revue périodique de la conformité du système à sa documentation technique.	Bonne pratique

	Risques	Objectifs du contrôle	Contrôles	Priorité
4. ENVIRONNEMENT DE TRAVAIL	Risque social et risque juridique du fait du Code du travail français et de l'application qui en fait par la jurisprudence qui considère que l'introduction d'une nouvelle technologie (tel qu'un logiciel d'IA) justifie à elle seule que le CSE puisse, solliciter une expertise externe, sans qu'il ne soit nécessaire de démontrer préalablement un impact sur les conditions de travail des salariés.	4.1. Le déploiement de systèmes algorithmiques s'effectue dans le respect du dialogue social. Jurisprudence.	4.1.1 S'assurer que l'introduction de chaque système algorithmique ayant des incidences sur l'environnement de travail a bénéficié d'une procédure d'information consultation auprès des instances représentatives du personnel, conformément à l'article L2112-8 du Code du travail.	Recommandé
	Le déploiement de SIA fait naître des risques psychosociaux qui peuvent grever la productivité de l'entreprise et conduire à des mouvements sociaux de contestation.	4.2 Les risques psychosociaux susceptibles de naître du déploiement de systèmes algorithmiques dans l'environnement de travail sont maîtrisés.	4.2.1 S'assurer que l'introduction de chaque système algorithmique ayant des incidences sur l'environnement de travail a fait l'objet d'une mesure d'évaluation préalable des risques psycho-sociaux qu'elle est susceptible d'entraîner.	Recommandé
			4.2.2 S'assurer de l'existence d'un plan de communication et d'acculturation des salariés affectés par le déploiement de système algorithmique.	Bonne pratique
			4.2.3 S'assurer de l'existence d'un plan de formation à destination des salariés utilisateurs ou encadrants de systèmes algorithmique.	Bonne pratique
			4.2.4 S'assurer de l'existence d'un plan d'évaluation continu pour chaque système algorithmique déployé dans l'environnement de travail et susceptible de faire naître des risques psychosociaux. Ce plan d'évaluation contient notamment des informations sur la productivité des salariés utilisateurs, sur la satisfaction des utilisateurs et sur les difficultés rencontrées.	Bonne pratique
			4.2.5 S'assurer que le dispositif d'alerte interne est ouvert aux salariés souhaitant rapporter des difficultés liées à la transformation de leur environnement de travail à la suite du déploiement d'un système algorithmique.	Bonne pratique
DONNÉES PERSONNELLES		Voir : Légalité du recueil, droit d'accès, de rectification et d'effacement, droit d'opposition, droit à la portabilité des données, principe de minimisation, transfert vers des pays tiers	Couvert par les process RGPD	Requis

INTELLIGENCE ARTIFICIELLE
ÉTHIQUE, RISQUES ET CONTRÔLE DES OUTILS POUR SE PRÉPARER AU RIA



Edition : Novembre 2024

IFACI
Elevating Impact

LE CERCLE D'ÉTHIQUE DES AFFAIRES

WWW.IFACI.COM

CONTACT :
Philippe MOCQUARD,
Délégué général de l'IFACI
p.mocquard@ifaci.com

WWW.CERCLE-ETHIQUE.NET

CONTACT :
Louis COLIN, Délégué général
du Cercle d'Éthique des Affaires
louis.colin@cercle-ethique.net