CPRS | SCRP

Trousse de vérification et de responsabilisation en IA

Des outils pratiques pour une utilisation responsable de l'IA en communications et en relations publiques

Octobre 2026

AVANT DE COMMENCER

Remerciements et divulgation

Dirigée par le Conseil des maîtres à penser de la Société canadienne des communications et des relations publiques (SCRP), cette trousse s'inspire de la publication AI and Digital Ethics for Communicators, produite du *Chartered Institute of Public Relations* et ses membres collaborateurs, Frank Dias (créateur principal), Courtney Ellul, Hina Sharma, Jenni Field, Andrew Hesselden, Fa Mafi, Amber Brittain, Nafisa Shafiq et Grace Park.

Publié en 2026, le document du CIPR est paru au moment même où le Conseil des maîtres à penser examinait les résultats de la consultation menée auprès des délégués lors du Congrès national 2026 à St. Andrews, au Nouveau-Brunswick. Les commentaires des professionnels des communications et des relations publiques étaient clairs : il fallait des balises pour encadrer l'adoption rapide de l'IA; il fallait mieux comprendre la divulgation et la vérification; et il fallait des outils pratiques plutôt que de nouvelles discussions sur la gouvernance.

Dans un souci de pleine transparence, précisons que cette trousse a été élaborée à l'aide de l'IA, en l'occurrence Claude CoWork et ChatGPT. La responsable principale a utilisé l'IA pour analyser les résultats de la consultation des délégués à la lumière de la publication du CIPR, pour examiner des études récentes et du contenu de leadership d'opinion (voir l'annexe 10), pour balayer l'environnement juridique canadien et pour structurer le document avant la rédaction. L'IA a servi à appuyer plusieurs versions du document et à synthétiser les commentaires des réviseurs. Une révision finale a été effectuée, et l'IA a contribué à la traduction du document vers le français.

Claude Design a aussi servi à orienter la mise en page finale du document dans Microsoft Word, en fournissant des instructions à la responsable principale (parce que, disons-le, on travaille avec un budget limité).

Voici le processus humain :

CLASSIFIER	Ce projet a été classé au niveau 3, soit le degré de supervision le plus élevé (voir la section 04). Toutes les données de consultation ont été dépouillées des identifiants, adresses courriel, noms et autres détails avant d'être analysées. Il était clair dès le départ que ce travail exigerait une révision et une supervision rigoureuses pour garantir l'exactitude et la qualité de la trousse.
INTERROGER	Des projets précis ont été montés dans les plateformes d'IA, avec des consignes et des exigences très strictes. Le document a été construit section par section, avec d'importants commentaires et corrections humaines avant de passer à la section suivante.
VÉRIFIER	Toutes les sources citées dans ce document ont été vérifiées par la responsable principale. Toutes les statistiques et informations ont été validées par les deux plateformes d'IA, puis repérées et confirmées manuellement par la responsable principale. Le document a été révisé par les personnes mentionnées dans le tableau ci-dessous. La traduction française a été révisée par Louis Payette, de ChangeMakers.

DIVULGUER Toutes les versions de travail indiquaient que l'IA avait été utilisée dans l'élaboration du document, de sorte que les réviseurs connaissaient les outils utilisés et savaient qu'ils examinaient des contenus assistés par l'IA ou générés par l'IA. Aucun contenu n'a été transmis aux réviseurs sans révision humaine préalable.

Remerciements particuliers à nos collaborateurs et réviseurs

CONSEIL DES MAÎTRES À PENSER

Colleen Killingsworth, MCM, ARP, FSCRP (présidente du Conseil)
Kim Blanchette, ARP, Chart.PR, FSCRP (responsable principale)
Lisa Covens, MSCRP, MA, CAIP
Sara Rafuse, MBA, CPF
Alex Sevigny, Ph. D., ARP, FSCRP
Christine Szustaczek, MCM, ARP, SCMP, FSCRP
Amy Thurlow, Ph. D., ARP, FSCRP
Martin Waxman, MCM, ARP, MSCRP

RÉVISEURS EXTERNES

Andrew Blanchette, MSCRP, vice-président principal, ChangeMakers
Andrea Sweet, vice-présidente principale, Castlemain/ChangeMakers
Louis Payette, directeur principal, Castlemain/ChangeMakers

Table des matières

01 Objectif et lien avec les lignes directrices de la SCRP

02 Le paysage juridique canadien

03 Notre rôle en matière d'éthique de l'IA

04 Vérifications éthiques

05 Outils de vérification et de responsabilisation

06 Arbre décisionnel de divulgation

07 À faire et à ne pas faire, par type de tâche

08 Scénarios

09 Liste de vérification pour bien démarrer

10 Annexe – Ressources

01 | OBJECTIF ET LIEN AVEC LES LIGNES DIRECTRICES SUR L'IA DE LA SCRP

Cette trousse se veut un complément aux Lignes directrices sur l'IA de la SCRP, approuvées par le conseil d'administration national de la SCRP en août 2026. Ces lignes directrices établissent sept grands principes pour une utilisation responsable de l'IA : transparence, exactitude et intégrité, protection de la vie privée, sécurité et consentement, équité et inclusion, supervision humaine, responsabilisation et avancement.

Cette trousse montre comment appliquer ces principes au travail quotidien et développe trois éléments que les Lignes directrices elles-mêmes engagent la SCRP à produire comme ressources complémentaires :

- des modèles de libellés de divulgation,
- des conseils pour la formulation des consignes à l'IA, et
- un outil d'autoévaluation pour la gouvernance organisationnelle de l'IA.

La SCRP a choisi de concevoir cet outil comme une trousse de vérification et de responsabilisation, et non comme une trousse de gouvernance.

C'est un choix délibéré.

Dans la lutte pour savoir qui « possède » la gouvernance de l'IA entre les TI, les affaires juridiques, la direction et les communications et relations publiques, la responsabilisation peut se perdre.

Les professionnels des communications et des relations publiques sont les gardiens de la réputation organisationnelle et corporative. Certaines décisions précises dans le flux de travail lié à l'IA, comme ce qui est vérifié avant d'être publié ou ce qui est divulgué et à qui, nous appartiennent. Nous avons toujours appliqué des normes rigoureuses de révision, de vérification et d'approbation à notre travail, peu importe qui (ou quoi) l'a rédigé.

La trousse comble un écart observé au cours des 18 derniers mois. En 2025, *l'étude de la SCRP sur l'état des relations publiques au Canada* a révélé que 90 % des professionnels canadiens estiment que l'IA doit être utilisée de façon éthique, mais que seulement 27 % déclarent disposer d'une politique d'IA bien établie et mise en œuvre au sein de leur organisation. Le sondage 2026 du Boston Consulting Group (BCG) auprès des dirigeants des Affaires publiques et Communications révèle le même constat : 88 % affirment ne pas être pleinement prêts à diriger une transformation liée à l'IA dans leur fonction.

Une étude de l'Institute for Public Relations a révélé que ce sont généralement les TI qui pilotent l'adoption de l'IA générative, mais que les professionnels des communications et des relations publiques jouent le rôle de traducteurs entre les équipes techniques et le reste de

l'organisation. Ce rôle de traducteur comporte ses propres responsabilités en matière de vérification et de divulgation.

> Comme l'a dit un membre de la SCRP lors du Congrès national à Banff : « on court avec l'IA avant même d'avoir appris à marcher avec une politique ».

Cette trousse a été adaptée, avec permission, du guide du groupe Inside du Chartered Institute of Public Relations (CIPR), AI and Digital Ethics for Communicators, et s'inspire d'autres pratiques exemplaires et contenus de leadership d'opinion provenant notamment de la Public Relations Society of America (PRSA) et de l'Institute for Public Relations (IPR). La liste complète des sources se trouve à la page 49.

Cette trousse nous fait passer à l'étape suivante en fournissant l'infrastructure et les balises nécessaires, que vous en soyez à vos premiers pas ou que vous cherchiez à améliorer un processus déjà en place.

Les choses évoluent rapidement, probablement plus vite que cette trousse ne pourra être mise à jour. Les professionnels des communications et des relations publiques sont invités à se tenir au fait des dernières tendances et des changements réglementaires.

La SCRP est membre de la Global Alliance for Public Relations and Communication Management et appuie l'Engagement de Venise de la Global Alliance pour une utilisation responsable de l'IA en relations publiques. Cette trousse a été conçue en cohérence avec cet engagement, afin de traduire les principes de l'Engagement de Venise en pratiques quotidiennes pour les membres de la SCRP.

02

Le paysage juridique canadien

“Les arguments en faveur de la vérification, de la responsabilisation et de règles claires en matière de divulgation gagnent du terrain, mais pas au rythme de l'adoption.”

02 | LE PAYSAGE JURIDIQUE CANADIEN

Il est important de comprendre ce qui encadre l'utilisation de l'IA pour les professionnels canadiens des communications et des relations publiques en 2026, et comment le droit fédéral s'articule avec les exigences provinciales, notamment au Québec.

Au fédéral, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) ne fait pas mention de l'IA en tant que telle. Le Commissariat à la protection de la vie privée du Canada (CPVP) est toutefois intervenu avec des principes conjoints pour une IA générative responsable, digne de confiance et respectueuse de la vie privée. Le CPVP a aussi rendu des conclusions directement liées à des systèmes d'IA : une conclusion de 2026 visant OpenAI (n° 2026-002) et une conclusion de 2026 visant X Corp et xAI concernant la génération d'hypertrucages par Grok (n° 2026-004).

La conclusion visant OpenAI découle d'une enquête conjointe menée avec les autorités de protection de la vie privée du Québec, de la Colombie-Britannique et de l'Alberta. Elle a révélé qu'OpenAI recueillait des renseignements personnels à une échelle dépassant ce qui était approprié, sans consentement valable, et n'avait pas vérifié si les renseignements personnels générés par ses modèles au sujet de personnes réelles étaient même exacts.

OpenAI s'est depuis engagée à mettre en place un nouvel outil de filtrage, des avis plus clairs et de meilleurs processus d'accès et de correction. Le régulateur fédéral a jugé ses conclusions résolues sous condition; la Colombie-Britannique et l'Alberta ont conclu que les exigences de consentement n'étaient toujours pas respectées. Leurs lois sont plus précises en matière de consentement, et les deux provinces ont jugé la pratique toujours non conforme. Pour les professionnels des communications et des relations publiques, cela a des répercussions bien réelles. Un outil aussi largement utilisé au sein des organisations, souvent sans aucune revue

La conclusion visant Grok est encore plus préoccupante. X et xAI ont lancé un outil de génération d'images sans avoir complété une évaluation des facteurs relatifs à la vie privée. En fait, cette évaluation n'a été terminée que plusieurs mois après le lancement.

Des reportages journalistiques et des chercheurs externes, cités dans la conclusion du Commissariat, estiment que Grok a servi à générer et à partager environ 1,8 million d'hypertrucages sexualisés non consensuels, dont plus de 23 000 représentant des enfants, selon une estimation du Center for Countering Digital Hate. Le CPVP n'a pas vérifié ces chiffres de façon indépendante.

Le Commissariat a recommandé de suspendre l'outil jusqu'à ce que des mesures de protection soient démontrées. Les entreprises ont refusé et affirment que la surveillance qu'elles ont plutôt ajoutée a réduit les incidents de moitié.

d'approvisionnement, a été jugé non conforme sur les deux aspects auxquels les praticiens tiennent le plus : le consentement et l'exactitude.

Devant l'intensification de la surveillance réglementaire, on trouve de plus en plus de ressources pour aider les professionnels des communications et des relations publiques à bâtir leur propre approche d'utilisation responsable de l'IA.

Plus précisément, les principes FASTER du Conseil du Trésor du Canada (équitable, responsable, sécurisé, transparent, éclairé, pertinent) et sa Directive sur la prise de décisions automatisée offrent des outils efficaces pour l'utilisation de l'IA dans le secteur public, qui peuvent éclairer les pratiques du secteur privé.

Le Québec va encore plus loin. Les modifications apportées par la Loi 25 à la Loi sur la protection des renseignements personnels dans le secteur privé imposent une obligation précise à l'égard des décisions automatisées, exigeant une divulgation et une explication chaque fois qu'un système automatisé prend une décision concernant une personne sans intervention humaine significative. Le Québec exige aussi la désignation d'un responsable de la protection des renseignements personnels et impose une structure de pénalités à deux volets : des sanctions administratives pécuniaires pouvant atteindre 10 millions de dollars (ou 2 % du chiffre d'affaires mondial, selon le montant le plus élevé) et des amendes pouvant atteindre 25 millions de dollars (ou 4 % du chiffre d'affaires mondial, selon le montant le plus élevé).

Les répercussions d'une IA sans balises dépassent largement les hallucinations ou l'embarras réputationnel qui en découle. Le rapport IBM Cost of a Data Breach 2025 a révélé qu'au Canada, les atteintes à la protection des données liées à l'IA fantôme, soit des outils utilisés sans approbation ni connaissance de l'organisation, entraînaient un coût supplémentaire moyen de 308 000 $ CA, et que 20 % des organisations étudiées avaient subi un incident de sécurité lié à l'IA fantôme. Une étude distincte commandée par IBM révèle que si 79 % des employés de bureau à temps plein utilisent l'IA au travail, seulement 25 % ont recours à des outils d'IA de niveau entreprise. Les autres utilisent une combinaison d'outils personnels et fournis par l'employeur (33 %) ou se fient entièrement à des applications personnelles (21 %). L'IA fantôme a été une préoccupation majeure lors des tables rondes du Congrès national 2026 de la SCRP à St. Andrews, au Nouveau-Brunswick, l'exposition non gérée des données étant la principale source d'inquiétude soulevée.

L'Atlas de la confiance envers l'IA 2026 de TELUS, produit avec Léger, révèle que 90 % des Canadiens souhaitent que l'IA soit réglementée, mais seulement 27 % ont confiance en la

pertinence des lois actuelles. Les arguments en faveur de la vérification, de la responsabilisation et de règles claires en matière de divulgation gagnent du terrain, mais pas au rythme de l'adoption.

03

Notre rôle en matière d'éthique de l'IA

“Quand la gouvernance de l'IA appartient à tout le monde, elle n'appartient à personne.”

03 | NOTRE RÔLE EN MATIÈRE D'ÉTHIQUE DE L'IA

Quand la gouvernance de l'IA appartient à tout le monde, elle n'appartient à personne.

Cela présente des risques pour les organisations et leurs publics. L'Atlas de la confiance envers l'IA 2026 de TELUS révèle que seulement 34 % des Canadiens font confiance aux entreprises qui utilisent l'IA. La même étude montre ce qui changerait ce chiffre : 76 % feraient davantage confiance à une entreprise si elle révisait activement ses systèmes d'IA pour en détecter les préjudices, 73 % si elle expliquait son utilisation de l'IA en langage clair, et 69 % si elle donnait au public un droit de regard sur la façon dont l'IA est utilisée.

La SCRP demande « la participation précoce et continue des professionnels des communications à l'élaboration, au déploiement et à la gouvernance de l'IA, afin d'évaluer les risques réputationnels, les considérations éthiques et les répercussions sur le public ».

Les cinq rôles décrits ci-dessous montrent comment cette participation peut se traduire au quotidien. Dans certains cas, notre rôle consiste à poser des questions et à faire remonter les enjeux plutôt qu'à exécuter. Ce qui compte, c'est que les professionnels des communications et des relations publiques établissent des relations de travail avec les fonctions responsables ou de soutien de chaque responsabilité.

Traducteur ou traductrice / Éducateur ou éducatrice

Responsable

Collabore avec : les TI (source des explications techniques)

Gardien ou gardienne de la confiance

Responsable

Collabore avec : les affaires juridiques

Détecteur ou détectrice de risques

Soutient et fait remonter les enjeux

Collabore avec : les TI, le responsable de la protection des renseignements personnels, les spécialistes en science des données ou éthiciens pour les travaux d'IA fondés sur la recherche; les analystes de données, pour la révision statistique ou méthodologique des résultats de l'IA

Facilitateur ou facilitatrice de la responsabilisation

Défend et applique

Collabore avec : le gouvernement, les affaires juridiques et les TI.

Facilitateur ou facilitatrice du changement et des compétences

Responsable à l'interne | défenseur.e à l'externe

Collabore avec : les RH, la formation et le perfectionnement

Traducteur ou traductrice / Éducateur ou éducatrice

Avant qu'un outil d'IA soit utilisé ou déployé plus largement dans votre organisation, les communications et relations publiques devraient être en mesure de l'expliquer en langage clair – ce qu'il fait, quelles informations il touche et ce qui pourrait mal tourner – aux dirigeants, aux employés ou aux médias.

Si l'organisation ne peut pas fournir cette explication, c'est probablement que l'outil n'est pas prêt à être utilisé. Cette fonction de traducteur se reflète dans l'étude de l'IPR : *les TI pilotent l'adoption; les communicateurs l'expliquent à tous les autres.*

Ce rôle exige aussi de surveiller les outils d'IA déjà utilisés que personne n'a officiellement approuvés. L'IA fantôme crée un véritable risque réputationnel, en plus de l'exposition en matière de sécurité.

Cette explication clôt rarement le dossier. Bien expliquer un outil pour que les gens lui fassent confiance tend à créer des besoins supplémentaires : une éducation continue sur l'outil lui-même, et sur ce qu'il change dans la façon dont les gens travaillent.

Gardien ou gardienne de la confiance

En s'appuyant sur les outils de cette trousse, les professionnels des communications et des relations publiques offrent des conseils à leur organisation sur l'opportunité et la façon de divulguer qu'un contenu a été assisté par l'IA. Dans bien des cas, il s'agit d'un jugement fondé sur le risque et l'impact. Mais au Québec, lorsqu'un système automatisé prend une décision concernant une personne sans intervention humaine significative, la loi exige la divulgation.

Ce rôle doit composer avec deux enjeux à la fois. D'un côté, sous-divulguer l'utilisation de l'IA risque d'induire un public en erreur, mais il en va de même pour la surdivulgation : qualifier une simple automatisation ou un outil de mise en forme d'« alimenté par l'IA » pour paraître à jour mine la confiance tout autant que de cacher un usage réel de l'IA.

Détecteur ou détectrice de risques

Le risque, ici, dépasse la protection de la vie privée, bien qu'elle demeure importante. Il englobe les biais, l'exactitude, la sécurité, l'exposition réputationnelle, ainsi que les enjeux de conformité et juridiques. Les professionnels des communications et des relations publiques peuvent repérer ces risques tôt, en posant à l'interne la question qui dérange avant que quelqu'un à l'externe ne la pose.

La plupart des évaluations des facteurs relatifs à la vie privée sont rédigées par les TI, la sécurité ou un responsable de la protection des renseignements personnels, et ne sont pas toujours révisées par les professionnels des communications et des relations publiques. Ici, le rôle consiste à soutenir et à poser les questions clés :

- l'information a-t-elle été vérifiée?
- une évaluation d'impact existe-t-elle pour cet usage?
- est-ce que cela poserait problème si c'était divulgué après coup?

La conclusion du CPVP visant Grok illustre le danger de compléter une évaluation des facteurs relatifs à la vie privée après le lancement, une fois le préjudice déjà survenu. Repérer les risques et travailler avec son organisation pour en gérer l'atténuation fait passer ce rôle au-delà de la conformité, vers des facteurs clés touchant la réputation et la confiance.

Lorsque l'IA touche à la recherche sur les publics ou les participants en particulier, les Principes directeurs pour l'utilisation de l'IA en recherche marketing du Conseil de recherche et d'intelligence marketing canadien (CRIC) recommandent une supervision multidisciplinaire, faisant appel à des data scientists, à des éthiciens et à une expertise juridique, en plus des communications.

Facilitateur ou facilitatrice de la responsabilisation

Les principes FASTER et la Directive sur la prise de décisions automatisée du Conseil du Trésor sont des cadres gouvernementaux, élaborés conjointement par les fonctions gouvernementales, juridiques et de TI. Les professionnels des communications et des relations publiques doivent veiller à ce que leur travail suive un processus clair d'évaluation, de vérification, d'approbation et de divulgation.

En pratique, cela signifie bâtir les gabarits, les listes de vérification et les étapes de révision qui rendent une utilisation éthique de l'IA reproductible, plutôt que tributaire de l'expertise de la personne qui reçoit le travail.

Si votre organisation dispose déjà d'une politique encadrant ces actions, tant mieux. Si ce n'est pas le cas, c'est ici que les professionnels des communications et des relations publiques ont la

responsabilité d'en réclamer une et de faire preuve de leadership en en établissant une pour la fonction communications, peu importe ce qui existe à l'échelle de l'organisation.

Facilitateur ou facilitatrice du changement et des compétences

L'adoption de l'IA est un parcours de changement continu. La façon dont elle est introduite, séquencée et mise en œuvre détermine si les gens lui font confiance ou y résistent. C'est là que les professionnels des communications et des relations publiques jouent un rôle clé.

Deux idées issues du leadership d'opinion canadien viennent renforcer l'importance de ce rôle.

Le modèle à quatre éléments du Dr Alex Sévigny sur la compétence des communicateurs, soit les données, puis la littératie en IA, puis les processus d'affaires, puis la gestion du changement, délibérément dans cet ordre, plaide contre le fait de commencer par les outils. Son modèle efficacité-efficience-rendement vérifie d'abord si l'IA fonctionne en contexte contrôlé, puis dans le monde réel, avant d'optimiser les coûts – un test utile tant pour ce rôle que pour celui de détecteur de risques.

Les professionnels des communications et des relations publiques doivent développer les compétences et le discernement nécessaires pour comprendre les outils, la façon dont ils sont adoptés au sein de leur organisation, et pour réduire les risques. Et nous devons le faire en tenant compte des pressions d'efficience et des réalités du contexte organisationnel. Nous ne devrions pas ériger d'obstacles, mais nous pouvons soutenir la transformation avec des conseils judicieux et une gestion pratique des risques.

> **Un mot sur la délégation cognitive**
>
> Les humains ont toujours délégué une partie de leur travail cognitif. On ne fait plus de calculs avec un boulier, et on ne demanderait pas non plus les plans d'une maison dessinés à la main. Les outils d'IA aident à déléguer une plus grande part de la réflexion par la rédaction, le résumé et, dans certains cas, la prise de décision. L'étude 2025 de Michael Gerlich, AI Tools in Society: Impacts on Cognitive Offloading and the Future of Critical Thinking a révélé qu'une dépendance accrue à l'IA prédit des scores de pensée critique mesurablement plus faibles, l'effet étant le plus marqué chez les participants plus jeunes, d'où l'importance d'accompagner le personnel moins expérimenté.

Pour le rôle de facilitateur du changement et des compétences, il s'agit autant d'une question de séquençage que d'éthique. Prévoyez des moments délibérés, en particulier pour les décisions à forte charge émotionnelle ou réputationnelle, où des échanges inclusifs et le partage des connaissances aident les gens à développer leur esprit critique plutôt que de laisser l'IA faire toute la réflexion.

04

Vérifications éthiques

« Quatre étapes intégrées pour travailler de façon éthique avec l'IA. »

04 | VÉRIFICATIONS ÉTHIQUES

Il y a quatre étapes intégrées pour travailler de façon éthique avec l'IA : classifier ce que vous faites, formuler vos consignes avec rigueur, vérifier selon la classification établie, puis divulguer.

Étape 1 : Classifier

Étape 1 : Classifier	Étape 2 : Formuler la consigne (SAR)	Étape 3 : Vérifier	Étape 4 : Divulguer

Classifiez avant de demander quoi que ce soit à l'IA. Comprenez ce que vous êtes sur le point de créer et le niveau de risque que cela représente pour votre organisation.

> Tout ce qui suit dans cette section suppose que la consigne elle-même ne contient ni identifiants personnels ni renseignements confidentiels. Si une tâche consiste à transmettre directement des renseignements personnels, des renseignements de santé ou des données organisationnelles confidentielles à un outil d'IA, vous devez vous arrêter, à moins de disposer d'un processus de protection de l'information approuvé par les TI et les affaires juridiques.

Par exemple, pour analyser des commentaires ou des réponses de consultation contenant des renseignements d'identification, vous devez dépersonnaliser ou anonymiser les données avant de les transmettre à l'outil. Ce processus doit être documenté et vérifiable.

La loi québécoise est très claire à ce sujet. Un renseignement dépersonnalisé ne permet plus d'identifier une personne directement; un renseignement anonymisé ne permet plus de l'identifier, ni directement ni indirectement, de façon irréversible. Confirmez l'exigence précise auprès de vos conseillers juridiques avant de vous fier à une méthode d'anonymisation pour tout usage qui dépasse le cadre interne courant.

Pour tout le reste, une approche par paliers vous aide à déterminer la marche à suivre. Six questions doivent être considérées pour évaluer un dossier :

? Est-ce destiné au public?	? Pourrait-il causer un préjudice si c'était erroné?
? Est-ce sensible?	? Serait-il difficile de faire marche arrière?
? Comporte-t-il des faits ou des chiffres sur lesquels quelqu'un s'appuiera?	? Déclencheur décision-données : le travail sert-il aussi à classer, noter ou recommander quelque chose, à éclairer ou à orienter une décision, ou contient-il des chiffres, des statistiques ou une interprétation de données?

Commencez au niveau 1. Chaque « oui » fait passer le dossier au niveau suivant, jusqu'à un maximum de niveau 3. Deux réponses « peut-être » comptent pour un « oui ». Un seul « oui », y compris à la question « est-ce destiné au public? », fait passer un contenu courant au niveau 2.

NIVEAU	QUAND IL S'APPLIQUE	CE QUE CELA SIGNIFIE
Niveau 1 : Léger	Travail interne à faible impact, sans réponse « oui »	Autovérification par la personne ayant utilisé l'outil
Niveau 2 : Standard	La majorité du travail quotidien en communications et relations publiques, avec une seule réponse « oui »	Un deuxième réviseur indépendant vérifie le résultat
Niveau 3 : Renforcé	Dossier comportant deux réponses « oui » ou plus. Par exemple, public et sensible, ou difficile à annuler et alimentant une décision	Prise en charge, ébauche par l'IA, révision, révision spécialisée, supervision, contrôle qualité final et registre de validation

Les Principes directeurs pour l'utilisation de l'IA en recherche marketing du CRIC appliquent la même logique à la recherche : la révision éthique devrait être proportionnelle à la portée, au risque et à l'impact potentiel.

Étape 2 : Formuler la consigne avec la méthode SAR



Une fois votre niveau établi, le CIPR propose la méthode SAR — *Setup, Ask, Refinement* (cadrage, demande, raffinement) — comme discipline pour la formulation même des consignes, selon le degré de rigueur exigé par ce niveau.

S **Setup (cadrage) :** protection de la vie privée et minimisation des données. Énoncez l'objectif réel plutôt qu'un objectif vague : un mandat précis produit une réponse précise. Ajoutez du contexte, mais arrêtez-vous à la limite de la vie privée. Au-delà de ce qui a déjà été discuté au sujet des renseignements personnels, veillez à retirer les noms de clients et les détails commercialement sensibles, selon les directives de votre organisation.

A **Ask (demande) :** exactitude et maîtrise de la portée. Précisez le format souhaité plutôt que de le laisser ouvert. Ancrez la demande dans vos propres sources : « utilisez uniquement l'information ci-dessous; si quelque chose manque, indiquez-le sous forme de question » réduit les détails inventés de façon plus fiable que de demander à l'outil de signaler ses propres hallucinations, ce qu'il ne peut pas faire de façon fiable. Fixez des limites contre le jargon, les statistiques inventées et le langage promotionnel, et découpez les demandes complexes en étapes plutôt que de tout demander d'un coup.

R **Refinement (raffinement) :** biais, suppositions et impact. Traitez la première réponse comme une ébauche, pas comme une réponse finale. Demandez quelles suppositions ont été faites et ce qui manque. Demandez à l'outil de se remettre en question : où cela pourrait-il être biaisé, quel point de vue manque-t-il, quel est le contre-argument le plus solide? Vous voudrez peut-être comparer les résultats de deux outils ou de deux tentatives pour cerner où une vérification supplémentaire s'impose.

Étape 3 : Vérifier

Étape 1 : Classifier	Étape 2 : Formuler la consigne (SAR)	**Étape 3 : Vérifier**	Étape 4 : Divulguer

La vérification est guidée par le niveau attribué à l'étape 1.

- Le niveau 1 correspond à une autovérification par la personne ayant utilisé l'outil.
- Le niveau 2 exige un deuxième réviseur indépendant, une personne autre que le rédacteur.
- Le niveau 3 exige la séquence de révision complète : prise en charge, ébauche par l'IA, révision, révision spécialisée, supervision, contrôle qualité final et registre de validation (voir l'exemple ci-dessous).

Si l'étape 1 a signalé un déclencheur décision-données, allez plus loin en vérifiant les données sous-jacentes avant de les utiliser, en recalculant les chiffres et en veillant à ce qu'une personne interprète la signification du résultat avant que quiconque n'agisse en conséquence.

Les Lignes directrices sur l'IA de la SCRP offrent à chaque membre une courte liste de vérification à suivre avant toute utilisation de l'IA. Les huit vérifications ci-dessous reprennent cette même idée et l'appliquent à un dossier précis, plus en détail. Chaque vérification est une question à se poser, avant et après la formulation de la consigne, ainsi qu'un signal d'alerte indiquant qu'il faut y regarder de plus près.

Objectif et avantage

Quel avantage cherchons-nous à offrir, et quel préjudice pourrait survenir si cela tourne mal?

Signal d'alerte : vous pouvez expliquer le gain d'efficience, mais pas qui en profite au-delà de votre propre équipe.

Données et vie privée

Quelles données sont utilisées, comprennent-elles des renseignements personnels ou sensibles, et existe-t-il une raison documentée de les utiliser ainsi?

Signal d'alerte : vous ne pouvez pas dire rapidement quelles données ont été transmises dans la consigne ou où elles se trouvent.

Exactitude et preuves

Qu'est-ce qui est vérifié par rapport à ce qui est généré, et qu'est-ce qui doit être validé avant publication?

Signal d'alerte : un résultat au ton assuré est jugé fiable simplement parce qu'il semble juste.

Biais et inclusion

Qui pourrait être exclu ou désavantagé? Existe-t-il un risque de stéréotypes dans les données ou le résultat?

Signal d'alerte : personne n'a demandé de quelle expérience le résultat rend compte. Lorsque le travail touche des données ou des communautés autochtones, appliquez une approche fondée sur les distinctions et validez la conformité avec des principes de souveraineté des données tels que PCAP® et CARE.

Transparence et divulgation

Quand et comment l'utilisation de l'IA devrait-elle être divulguée, et à quoi le public s'attendrait-il raisonnablement?

Signal d'alerte : vous seriez mal à l'aise d'expliquer votre utilisation de l'IA au public après coup.

Supervision humaine

Qui est responsable du résultat final, et une personne l'a-t-elle révisé avant publication?

Signal d'alerte : vous ne pouvez pas nommer qui en répondrait si les choses tournaient mal demain. L'Atlas de la confiance envers l'IA de TELUS révèle que 60 % des Canadiens jugent la supervision humaine essentielle, peu importe la tâche, et que l'aisance à l'égard des décisions de santé prises par l'IA passe de 39 % à 63 % dès qu'une supervision humaine est confirmée.

Propriété intellectuelle et droits

Le droit d'auteur, les licences et la propriété sont-ils respectés, et le résultat pourrait-il porter atteinte à la propriété intellectuelle d'autrui?

Signal d'alerte : personne n'a vérifié les conditions d'utilisation de l'outil quant à la propriété du résultat.

Sécurité et usage abusif

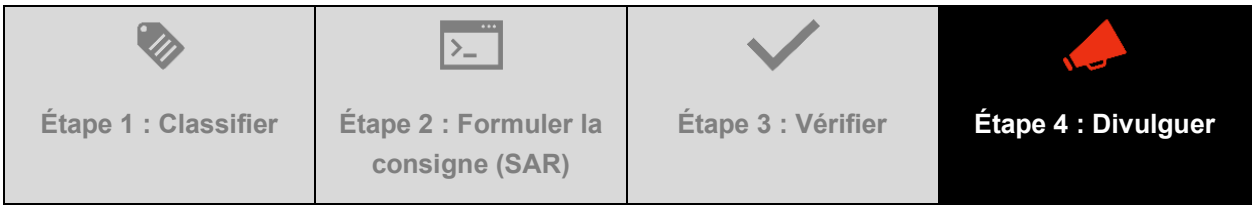
Cela pourrait-il être exploité à des fins d'usurpation d'identité, d'hameçonnage, de fuite de données ou de préjudice réputationnel?

Signal d'alerte : personne n'a demandé ce qui se passerait si cela tombait entre de mauvaises mains.

Chaque niveau exige des vérifications différentes. Le tableau ci-dessous offre des indications selon la classification établie à l'étape 1.

NIVEAU	QUAND IL S'APPLIQUE
Niveau 1 : Léger	Exactitude, divulgation, supervision humaine, données et vie privée, comme norme de base.
Niveau 2 : Standard	Exactitude, divulgation, supervision humaine, données et vie privée, plus les autres vérifications pertinentes parmi les quatre restantes selon la tâche.
Niveau 3 : Renforcé	Les huit.

Étape 4 : Divulguer



La vérification confirme que le travail est juste. La divulgation confirme que votre public sait comment il a été produit, et vous procure une trace à laquelle vous référer si on vous pose la question.

Chaque registre devrait consigner quatre éléments :

Objectif d'affaires. Ce que le professionnel cherchait à accomplir.	Intrants. Quelle information et quelles consignes l'IA a reçues : demandes, sources, autres intrants.	Mise à l'essai. Comment le résultat a été testé et transformé avant d'être utilisé.	Responsabilisation. Qui a assumé la responsabilité de la communication finale, et quand.

Il s'agit d'une approche de base et vérifiable, appelée à évoluer à mesure que les normes de divulgation se préciseront.

Suivi : un registre simple permet de suivre chaque livrable assisté par l'IA tout au long de son cycle de révision. Une version plus détaillée peut aussi inclure un hyperlien vers chaque étape de l'ébauche (ébauche par l'IA, première révision humaine, révision finale), une cote de qualité du résultat, et une indication à savoir si l'élément est passé à un flux de production ou de contrôle qualité plus large. Ajoutez des colonnes selon l'évolution de vos besoins de suivi.

N° DE REGISTRE	RÉSULTAT	OUTIL	DATE DE CRÉATION	CRÉATEUR OU CRÉATRICE	RÉVISEUR OU RÉVISEURE	DATE DE RÉVISION	APPROUVÉ	NOTES
1	[Nom du livrable]	[Outil d'IA]	[Date]	[Nom/rôle]	[Nom/rôle]	[Date]	[Oui/Non/En attente]	[Notes]

Vous pensez déjà que cela prend trop de temps? Compte tenu des gains d'efficience offerts par ces outils, quelques instants consacrés au suivi de vos résultats et de votre processus de révision pour les dossiers à risque plus élevé représentent un petit investissement dans votre réputation.

Pour le jugement au cas par cas sur l'opportunité et la façon de divulguer, voir l'arbre décisionnel de divulgation (section 6).

Et si...?

Ces étapes peuvent sembler abstraites tant qu'elles ne sont pas rattachées à un dossier précis. Voici quelques scénarios que pourraient vivre les professionnels des communications et des relations publiques :

Vous résumez des commentaires de consultation, de sondage ou de parties prenantes dans une note d'information ou un sommaire exécutif. Déclencheur : comporte des faits sur lesquels quelqu'un s'appuiera; peut toucher un sujet sensible **À faire :** Appliquez le filtre décision-données : vérifiez les données sources avant de les utiliser et confirmez la position en matière de protection de la vie privée si les réponses contiennent des renseignements personnels.	**Vous compilez des chiffres de rendement de campagne ou médiatique — portée, engagement, couverture, taux de clics — pour un rapport destiné à un client ou à la direction.** Déclencheur : comporte des faits ou des chiffres sur lesquels quelqu'un s'appuiera **À faire :** Recalculez les chiffres plutôt que de tenir pour acquis ceux fournis par l'IA. C'est probablement le scénario de niveau 2 le plus courant auquel les communicateurs feront face au quotidien.
Vous demandez à l'IA de classer ou de recommander le contenu, le message ou le canal ayant le mieux performé, pour orienter la suite du budget ou des efforts. Déclencheur : pourrait causer un préjudice si c'est erroné; difficile à annuler **À faire :** Traitez le classement comme une aide à la décision, non comme un fait. Un deuxième réviseur en vérifie la logique avant qu'il n'oriente une décision.	**Un mémoire ou un rapport que vous produisez pourrait éclairer une décision d'admissibilité, de financement, de politique ou de programme.** Déclencheur : pourrait causer un préjudice si c'est erroné; difficile à annuler **À faire :** Ce dossier passe au niveau 3 : Renforcé. Si le travail s'adresse au gouvernement ou à un client, vérifiez si la Directive sur la prise de décisions automatisée s'applique.

Une statistique ou un résumé généré par l'IA semble juste, et il n'y a pas le temps de vérifier la source avant son intégration dans une note d'information ou un document public.

Déclencheur : comporte des faits ou des chiffres sur lesquels quelqu'un s'appuiera

À faire : C'est exactement le scénario pour lequel le filtre décision-données existe. Vérifiez avant de vous y fier : plausible n'équivaut pas à vérifié.

05

Outils de vérification et de responsabilisation

« Des outils à commencer à utiliser dès aujourd'hui. »

05 | OUTILS DE VÉRIFICATION ET DE RESPONSABILISATION

Les Lignes directrices sur l'IA de la SCRP demandent déjà à chaque organisation de mettre en place quatre éléments :

Une liste d'outils approuvés	Un processus de révision et d'approbation	Une voie d'escalade	Une politique de base sur l'utilisation de l'IA

Cette section transpose ces quatre éléments en sept composantes concrètes que vous pouvez utiliser dès aujourd'hui. Les composantes une à cinq sont présentées ci-dessous; les composantes six et sept se poursuivent à la section 6 (l'arbre décisionnel de divulgation) et à la section 7 (à faire et à ne pas faire, par type de tâche). Si vous n'avez pas encore ces quatre bases, commencez par les mettre en place. Si vous les avez déjà, commencez par les trois premières composantes ci-dessous.

1 Balises de divulgation

Déterminez dès maintenant votre approche et votre libellé de divulgation. Constituez une petite bibliothèque de mentions de divulgation préapprouvées pour les scénarios récurrents de votre équipe : mises à jour internes, contenu externe, livrables clients, afin que personne n'ait à rédiger de libellé de divulgation à partir de zéro, et que tout le monde comprenne ce que la divulgation signifie en pratique.

> À surveiller : le Code de bonnes pratiques de l'Union européenne sur le marquage et l'étiquetage des contenus générés par l'IA établit un ensemble normalisé de pictogrammes de divulgation pour l'IA générative, lié aux exigences de transparence de l'article 50(4) du règlement européen sur l'IA visant les hypertrucages et les contenus générés par l'IA sur des questions d'intérêt public. Bien que non contraignant au Canada, un certain nombre d'organisations internationales y ont adhéré. L'approche par pictogrammes constitue une solution de rechange intéressante aux mentions de divulgation strictement textuelles, en particulier lorsque le contenu est généré sans révision humaine.

2 Règles de traitement des données

Appuyez-vous sur l'étape Classifier et les lignes directrices sur les renseignements personnels pour établir vos règles de base. Les données personnelles, les données clients et les renseignements confidentiels ou commercialement sensibles ne doivent pas être transmis dans une consigne à l'IA, à moins d'être anonymisés ou que l'outil ne soit spécifiquement approuvé pour cette catégorie de données.

3 Étapes de révision et d'approbation

Appuyez-vous sur l'approche par niveaux pour construire vos étapes d'approbation. La règle la plus simple? Personne n'approuve son propre résultat d'IA à partir du niveau 2.

4 Règles d'escalade

Des personnes-ressources désignées en protection de la vie privée, affaires juridiques, RH, sécurité et données/analytique, avec des déclencheurs clairs sur quand et comment faire remonter un dossier, par exemple lorsque des données personnelles ou sensibles sont en cause, qu'il y a un risque réputationnel, que le contenu s'adresse à l'externe, que des questions statistiques ou méthodologiques se posent, ou pour tout ce qui relève du niveau 3.

5 Liste des outils approuvés et de leur usage prévu

Un tableau simple nommant chaque outil approuvé, l'usage pour lequel il est approuvé et les limites de données applicables. Nommez un responsable pour cette liste ainsi que pour la liste d'escalade de l'élément 4, afin que les deux demeurent à jour. Révisez et mettez à jour au moins chaque trimestre, ainsi qu'à chaque changement d'outil, de modèle, de contrat ou de pratique de gestion des données. Pour tout fournisseur d'IA tiers, appliquez la norme de diligence raisonnable du CRIC : examinez les politiques de sécurité et l'état de conformité du fournisseur avant l'approbation, et documentez le protocole de transmission des données entre vos systèmes et les siens.

OUTIL	APPROUVÉ POUR	LIMITES DE DONNÉES
[Nom de l'outil]	[p. ex. premières ébauches, résumés internes]	[p. ex. aucune donnée client ou personnelle]
[Nom de l'outil]	[p. ex. approuvé pour le travail destiné aux clients]	[p. ex. entente d'entreprise en place]

06

Arbre décisionnel de divulgation

« Indice : dans le doute, divulguez »

06 | ARBRE DÉCISIONNEL DE DIVULGATION

La divulgation a été la préoccupation la plus constamment soulevée lors des tables rondes du Congrès national 2026 de la SCRP.

Les Lignes directrices sur l'IA de la SCRP sont claires : « Dans le doute, divulguez. La transparence est le point de départ de l'utilisation de l'IA, pas une solution de repli. » Elles distinguent ensuite trois contextes de divulgation :

- **Usage interne :** informez collègues et gestionnaires lorsque l'IA a façonné une ébauche, une analyse ou une décision sur laquelle ils s'appuient;
- **Travail client :** divulguez lorsque l'apport de l'IA est significatif pour la prise de décision du client ou l'acceptation du livrable, et posez la question dans le doute; et
- **Contenu destiné au public :** divulguez chaque fois que l'apport de l'IA pourrait raisonnablement influencer la réception du message ou la confiance qu'on lui accorde.

Se tromper dans un sens comme dans l'autre génère des répercussions. Trop divulguer sème le chaos dans le travail courant, tandis que ne pas assez divulguer risque d'induire les gens en erreur.

Le test de confiance en quatre questions ci-dessous vous aide à prendre ces décisions sur le vif.

1 **Ce contenu est-il partagé avec quelqu'un d'autre que vous, même de façon informelle, à l'interne, à l'externe, avec un client ou publiquement?**

Si non, consignez-le seulement à l'interne. Aucune divulgation requise.	**Si oui, passez à l'étape 2.**

2 **L'IA a-t-elle façonné le contenu, l'analyse ou la recommandation? Une simple mise au point (correction orthographique, mise en forme ou légère suggestion que vous révisez et pourriez facilement rejeter) ne compte pas.**

Si non, aucune divulgation requise. Documentez l'utilisation de l'IA à l'interne.	**Si oui, passez à l'étape 3.**

3 **Y a-t-il une personne responsable nommée qui a révisé le résultat de façon substantielle et en a accepté la responsabilité?**

Divulguez	**Si oui, passez à l'étape 4.**

4 **Une personne raisonnable parmi le public se sentirait-elle trompée si elle apprenait plus tard que l'IA a façonné ce contenu?**

Si non, la divulgation n'est pas requise. Documentez le raisonnement derrière la décision.	**Divulguez**

Au Québec, lorsqu'un système automatisé prend une décision concernant une personne en se fondant exclusivement sur un traitement automatisé, l'article 12.1 de la Loi sur la protection des renseignements personnels dans le secteur privé exige une divulgation et une explication, peu importe la conclusion des quatre questions ci-dessus.

Un libellé de divulgation utile couvre quatre éléments : l'outil utilisé, à quoi il a servi, comment le résultat a été vérifié, et qui l'a révisé.

[Nom de l'outil] a été utilisé pour rédiger [quoi], vérifié par [méthode], et révisé par [nom/rôle] avant publication.

Restez précis. Une mention vague du type « l'IA a contribué à ceci » laisse trop de zones grises et passe sous silence la révision et la vérification humaines.

Une complication à considérer

Une étude vient nuancer l'approche « dans le doute, divulguez ».

L'étude 2025 de Schilke et Reimann a mené 13 expériences portant sur la façon dont les gens jugent des superviseurs, des subordonnés, des professeurs, des analystes, des créatifs et des fonds d'investissement, et a révélé que la divulgation de l'utilisation de l'IA réduit la confiance par rapport à l'absence de divulgation ou à l'affirmation qu'un humain a fait le travail, peu importe le libellé de la divulgation, qu'elle soit volontaire ou obligatoire, ou que l'évaluateur sache déjà que l'IA était en cause.

L'étude de Schilke et Reimann laisse croire qu'être démasqué pour avoir caché l'utilisation de l'IA nuit encore plus à la confiance que de la divulguer d'emblée. Le choix pratique consiste moins à « subir un coup plus petit maintenant » qu'à adapter la divulgation aux attentes du public, à l'importance de l'enjeu, et à toute obligation légale ou politique applicable. La pénalité est légèrement moindre chez les personnes déjà favorables à la technologie, mais elle n'est pas atténuée par le degré de familiarité d'une personne avec l'IA ni par sa propre utilisation de l'IA.

Ce risque pourrait s'estomper avec le temps. Comparé au coût d'être démasqué plus tard, l'argument en faveur de la divulgation immédiate tient toujours, et une divulgation jumelée à une utilisation véritablement responsable devrait permettre de regagner la confiance à mesure que l'utilisation de l'IA se normalise.

La façon dont vous divulguez importe autant que le fait de divulguer. L'Atlas de la confiance envers l'IA 2026 de TELUS révèle que 73 % des Canadiens sont plus enclins à faire confiance à une entreprise qui explique son utilisation de l'IA en des termes qu'ils comprennent.

07

À faire et à ne pas faire, par type de tâche

07 | À FAIRE ET À NE PAS FAIRE, PAR TYPE DE TÂCHE

Les Lignes directrices sur l'IA de la SCRP classent l'utilisation de l'IA en trois catégories :

- usage approprié,
- usage à faire avec prudence, et
- usage à proscrire.

Les six types de tâches ci-dessous montrent à quoi cela ressemble dans les formats précis que produisent quotidiennement les professionnels des communications et des relations publiques.

Rédaction de communications

Courriels, publications sur les réseaux sociaux, articles intranet, scénarios et autres contenus rédigés.

Astuce rapide : ajoutez une ligne standard à votre consigne : « Vérifiez les faits, les noms et les chiffres, et citez vos sources dans la mesure du possible. »

À FAIRE

- Utilisez uniquement des outils et des sources de données approuvés.
- Retirez les détails sensibles avant de formuler votre consigne : données personnelles, noms de clients, données financières internes, renseignements commercialement sensibles.
- Précisez clairement quelles données l'IA doit ou ne doit pas utiliser.
- Faites réviser et valider chaque livrable de niveau 2 et 3 par une deuxième personne.
- Effectuez une vérification du langage clair et de l'inclusion pour tout contenu à forte visibilité.
- Lorsque le contenu est bilingue, effectuez une vérification d'équivalence en français, et non une simple passe de traduction. Une traduction techniquement exacte peut tout de même manquer le ton, l'idiome ou le sens.

À NE PAS FAIRE

- Coller des documents confidentiels dans des outils d'IA gratuits ou non approuvés sans avoir confirmé des protections de niveau entreprise liées au contrat et à la revue de gestion des données de votre organisation; si seule une version grand public est offerte, vérifiez d'abord ses paramètres de données et de confidentialité.
- Publier du contenu généré par l'IA sans en vérifier les faits, les statistiques, les références aux politiques ou les citations.
- Utiliser des outils d'IA personnels pour du contenu professionnel. Respectez la politique d'utilisation acceptable de votre organisation.

Résumer des réunions et des transcriptions

Astuce rapide : si vous partagez des notes générées par l'IA, ajoutez une ligne : « Résumé assisté par l'IA. La personne responsable de la réunion devrait confirmer les décisions à partir de l'enregistrement ou des notes originales. »

À FAIRE

- Confirmez que votre milieu de travail ou votre relation client permet l'enregistrement et la transcription avant de commencer.
- Traitez les résumés générés par l'IA comme des ébauches devant être révisées par défaut, et non comme des comptes rendus définitifs.
- Confirmez les décisions et mesures clés avec la personne responsable de la réunion et conservez vos propres notes en complément du résumé de l'IA.
- Stockez les résumés avec les bonnes autorisations d'accès, particulièrement pour les réunions avec des clients.

À NE PAS FAIRE

- Partager largement des résumés à diffusion restreinte « par commodité ».
- Traiter un résumé de l'IA comme le compte rendu définitif sans révision humaine.

Écoute des publics, analyse de sentiment et sondages éclair

Astuce rapide : ajoutez une mention partout où ces données sont partagées : « Thèmes indicatifs, et non une mesure définitive de l'intention individuelle. »

À FAIRE

- Expliquez ce qui est analysé et pourquoi.
- Agrégez les données dans la mesure du possible et minimisez les renseignements personnels dans les résultats.
- Vérifiez la présence de biais : qui est surreprésenté ou sous-représenté dans ce que vous analysez?
- Si l'IA interagit directement avec des personnes (clavardeurs, sondages adaptatifs), indiquez-leur clairement qu'elles s'adressent à une IA et non à une personne, et divulguez toute donnée ou tout profil synthétique utilisé, ainsi que son ampleur.

À NE PAS FAIRE

- Utiliser l'IA pour déduire des attributs personnels sensibles, comme la santé, les opinions politiques ou l'origine ethnique, sans consentement.
- Présenter le résultat de l'IA comme une « vérité » plutôt qu'un « signal ». Il nécessite toujours un jugement et une vérification humains.
- Laisser croire à quelqu'un, de façon raisonnable, qu'un système d'IA est un intervieweur ou un modérateur humain.
- Présenter des constats tirés de profils ou de données synthétiques comme s'ils provenaient de répondants réels.

Trousses pour gestionnaires, scénarios et FAQ

Astuce rapide : élaborez une FAQ d'une page pour les gestionnaires, avec quatre sections : messages clés, questions probables, voies d'escalade et rôle du gestionnaire.

À FAIRE

- Donnez aux gestionnaires ce dont ils ont besoin : ce qui est connu, ce qui ne l'est pas, quoi dire, où faire remonter un dossier, et leur rôle précis.
- Planifiez la diffusion pour réduire le bruit et maintenir une seule source fiable d'information.
- Testez les messages auprès d'un petit groupe avant une diffusion à grande échelle, particulièrement entre régions ou groupes linguistiques.

À NE PAS FAIRE

- Inonder les canaux de mises à jour fréquentes qui ajoutent de l'anxiété plutôt que de la clarté.
- Présumer qu'un message se diffusera fidèlement sans directives claires ni voie d'escalade.
- Garder pour soi les constats sur la réception des messages. Intégrez plutôt les commentaires des gestionnaires et des employés dans la prochaine ronde.

Charte d'équipe sur l'IA et discours « comment nous utilisons l'IA ici »

Astuce rapide : en équipe, rédigez une courte liste « ce que nous ferons et ne ferons pas avec l'IA ». C'est un moyen plus rapide de bâtir la confiance qu'une politique formelle.

À FAIRE

- Rédigez pour inspirer confiance : responsabilisation claire, limites claires, voies de soutien claires.
- Publiez un énoncé simple sur « l'utilisation de l'IA en communications », couvrant ce que vous faites et ne faites pas avec l'IA.
- Incluez une voie de recours : ce qu'une personne peut faire si elle n'est pas d'accord avec un résultat influencé par l'IA.
- Pour les équipes d'agence, confirmez quelle politique d'IA régit le travail client — la vôtre ou celle du client — avant la publication de la charte. Les contrats clients abordent de plus en plus cette question directement; vérifiez donc l'entente en vigueur plutôt que de présumer.

À NE PAS FAIRE

- Promettre une certitude excessive (« l'IA va tout régler »).
- Cacher l'apport de l'IA lorsque le public s'attendrait raisonnablement à une divulgation.
- Balayer du revers de la main les préoccupations des gens à l'égard de la sécurité d'emploi, de l'impact environnemental ou d'autres enjeux liés à l'IA. Faites plutôt appel à quelqu'un en mesure d'y répondre.

Automatisation des flux de travail courants en communications

Tâches récurrentes où l'IA peut faire économiser un temps réel : rédaction de mises à jour sur l'état d'avancement, planification et adaptation de publications sur les réseaux sociaux, assemblage d'infolettres, tri des demandes reçues, premières ébauches de comptes rendus de réunion, étiquetage et acheminement des mentions médiatiques.

Astuce rapide : pour chaque automatisation, répondez aux questions suivantes : qui en est responsable, qu'est-ce qui déclenche une révision humaine, et comment sauriez-vous qu'elle a fait défaut?

À FAIRE

- Commencez par des tâches à volume élevé, à faible risque et reproductibles, où une personne révise tout de même le résultat avant sa diffusion. Cette approche adapte à vos propres flux de travail le cadre à faible risque du Conseil du Trésor.
- Cartographiez le flux de travail de bout en bout avant d'en automatiser une étape.
- Maintenez une personne responsable nommée pour chaque flux de travail automatisé, même lorsque l'IA effectue la majorité du travail.
- Intégrez un mécanisme d'arrêt à chaque flux de travail : un signal (sujet sensible, plainte, anomalie) qui ramène une personne dans la boucle.
- Révisez les automatisations chaque trimestre. Les outils, les consignes et le matériel source évoluent tous avec le temps.

À NE PAS FAIRE

- Automatiser quoi que ce soit touchant une décision réglementée, un congédiement, une plainte ou un sujet sensible sur le plan émotionnel, sans point de contrôle humain explicite.
- Enchaîner des outils (l'IA rédige, l'IA publie, l'IA répond) sans point de contrôle humain quelque part dans la chaîne.
- Laisser une automatisation fonctionner sans supervision après le départ de la personne qui l'a créée. Les automatisations orphelines sont une cause fréquente de défaillances silencieuses.

08

Scénarios

« À utiliser pour des discussions d'équipe, des séances de formation ou une réflexion personnelle »

08 | SCÉNARIOS

Utilisez ces scénarios pour des discussions d'équipe, des séances de formation ou une réflexion personnelle lorsqu'une situation semblable se présente.

L'IA a rédigé le message de notre PDG

SITUATION

Une ébauche du message trimestriel du ou de la PDG à l'ensemble du personnel a été générée par l'IA, puis légèrement révisée. Le texte se lit bien. On vous demande de l'approuver.

POINTS À VÉRIFIER

Les affirmations, les chiffres et les engagements sont-ils vérifiés par rapport aux sources? Le ton reflète-t-il vraiment cette personne dirigeante, et non une voix générique de direction? A-t-elle autorisé le recours à l'IA pour rédiger des messages émis en son nom? Le public se sentirait-il trompé en apprenant que l'IA l'a rédigé?

MESURES À PRENDRE

Vérifiez les faits et les engagements nommés avant l'approbation, désignez une personne responsable à la fois des mots et des engagements qu'ils contiennent, et conservez l'ébauche et la trace de l'approbation conformément à la politique de conservation des documents de votre organisation.

PRINCIPE

La confiance chute lorsque les gens sentent qu'un message manque d'authenticité, peu importe d'où vient la première ébauche.

Nous voulons que l'IA analyse les commentaires ouverts d'un sondage

SITUATION

La direction souhaite que l'IA effectue une analyse thématique des réponses ouvertes d'un sondage de mobilisation. Cela peut se faire en quelques minutes, mais la rapidité n'équivaut pas à l'exactitude.

POINTS À VÉRIFIER

Y a-t-il des données personnelles, et le cas échéant, quel est le fondement légal de leur utilisation et quelle est la période de conservation? Quels groupes sont surreprésentés ou sous-représentés dans l'ensemble de données? A-t-on informé les répondants, en langage clair, que l'IA analysera leurs commentaires? Ont-ils un moyen de refuser l'analyse de leurs commentaires par l'IA ou de demander une révision humaine?

MESURES À PRENDRE

Agrégez les données par défaut et minimisez les renseignements personnels dans les résultats, publiez une brève explication de ce qui est analysé et pourquoi, et indiquez les limites dans tout rapport plutôt que de présenter les thèmes comme des faits. Lorsque des commentaires touchent des

sujets sensibles ou pénibles, acheminez-les à une personne réviseure nommée plutôt qu'à l'IA seule, et déterminez qui traitera une plainte d'un participant, le cas échéant.

PRINCIPE

L'IA peut repérer des tendances, mais c'est votre jugement qui détermine si cette tendance est réelle et si elle importe.



Nous devons expliquer notre utilisation de l'IA au public

SITUATION

Un service destiné à la clientèle utilise l'IA, et on vous a demandé de rédiger le message public à ce sujet.

POINTS À VÉRIFIER

Une personne non initiée peut-elle vous le reformuler avec exactitude? Décrivez-vous précisément ce que fait l'IA? Si la décision est automatisée, que se passe-t-il? L'entreprise en assumera-t-elle la responsabilité?

MESURES À PRENDRE

Rédigez une explication « comment ça fonctionne » couvrant ce que fait l'IA, quelles données elle utilise, le rôle de la supervision humaine, et le recours en cas de problème, puis testez-la auprès d'une personne non initiée avant de la publier.

PRINCIPE

Si vous ne pouvez pas l'expliquer en langage clair, vous n'êtes pas prêt à le déployer.

Le clavardeur qui a fait une promesse

SITUATION

Votre clavardeur transmet une information erronée à un client, qui agit en conséquence.

POINTS À VÉRIFIER

« C'est le clavardeur qui l'a dit » ne constitue pas une défense — un tribunal de la Colombie-Britannique a tenu Air Canada responsable exactement dans ce genre de situation, après que son clavardeur eut mal énoncé une politique de tarif de compassion (Moffatt c. Air Canada, 2024 BCCRT 149).

MESURES À PRENDRE

Le clavardeur a-t-il été testé par rapport à la politique réelle, y compris pour les sujets sensibles? Une voie d'escalade humaine était-elle prévue pour les questions à enjeux élevés? Le client savait-il qu'il s'adressait à une IA?

PRINCIPE

Traitez votre clavardeur comme tout autre porte-parole.

Regard de plus près : les clavardeurs en tant qu'agents IA

Le scénario ci-dessus traite le clavardeur comme une simple mauvaise réponse isolée. En pratique, bon nombre de clavardeurs destinés à la clientèle sont désormais des agents IA : ils conservent la mémoire d'une conversation, décident quoi demander ensuite et posent parfois des gestes (réservation, remboursement, escalade) sans qu'une personne n'approuve chaque étape. Appliquez ici les mêmes vérifications qu'à tout agent IA : une personne responsable nommée, une voie d'escalade testée pour les sujets sensibles, et la divulgation du fait que le public s'adresse à une IA, et non à une personne.

Nous l'utilisons discrètement depuis un moment

SITUATION

Une équipe utilise l'IA depuis des mois pour la rédaction, la recherche et l'analyse. Rien n'a été caché, mais rien n'a été divulgué non plus, et la direction souhaite maintenant prendre un engagement public envers une utilisation responsable de l'IA.

POINTS À VÉRIFIER

Pouvez-vous décrire fidèlement l'usage actuel à la direction? Comment l'équipe réagira-t-elle si la divulgation se fait sans sa participation?

MESURES À PRENDRE

Dressez le portrait de l'usage actuel avant de le présenter à qui que ce soit, divulguez d'abord aux parties prenantes internes avant les externes, et bâtissez la gouvernance pour l'avenir plutôt que rétroactivement.

PRINCIPE

Une adoption discrète demeure une adoption. Plus on attend avant de la nommer, plus il y aura à expliquer plus tard.

Notre agence a utilisé l'IA pour rédiger nos textes

SITUATION

Vous découvrez qu'une agence avec laquelle vous travaillez depuis longtemps utilise l'IA dans des travaux facturés comme s’ils étaient produits sur mesure. Le contrat n'aborde la question ni dans un sens ni dans l'autre.

POINTS À VÉRIFIER

Que dit, ou ne dit pas, votre entente sur l'utilisation de l'IA et la responsabilisation? Le travail était-il de qualité, et si oui, la préoccupation est-elle une question de principe ou de coût?

MESURES À PRENDRE

Ajoutez une clause sur l'utilisation de l'IA aux contrats de vos fournisseurs au prochain renouvellement, précisant ce qui doit être divulgué et quand, puis vérifiez dès maintenant vos principaux fournisseurs, même si vous n'avez pas encore toutes les réponses.

PRINCIPE

L'utilisation de l'IA par vos fournisseurs et agences demeure de votre responsabilité.

Puis-je coller ceci dans l'IA?

SITUATION

Il est tard, vous avez trois textes à rédiger ou à résumer rapidement, et l'outil d'IA gratuit dans votre navigateur pourrait tout faire en quelques minutes.

POINTS À VÉRIFIER

De quelle catégorie de données s'agit-il : publiques, internes, confidentielles ou réglementées? Quel niveau d'outil utilisez-vous, entreprise approuvée, abonnement d'affaires révisé, ou outil grand public gratuit? Si cela fuitait demain, pourriez-vous revenir en arrière?

MESURES À PRENDRE

Par défaut, oui pour les données publiques dans des outils approuvés; pour les données internes, confirmez d'abord qu'elles ne sont ni confidentielles, ni sensibles, ni assujetties à une restriction contractuelle. Par défaut, non pour les données confidentielles ou réglementées dans tout outil non approuvé, et dans le doute, suivez le processus de dépersonnalisation ou d'anonymisation de la section 4 plutôt que de simplement retirer les noms et les chiffres.

PRINCIPE

La question n'est pas de savoir si l'IA est sécuritaire. C'est de savoir si ces données, dans cet outil, pour cette tâche, le sont.

Notre IA a dévié du scénario

SITUATION

Un outil marketing doté de fonctions agentiques, capable de chercher, de rédiger, de publier et de répondre par lui-même, fonctionne sans supervision depuis des semaines. Il fait du bon travail, jusqu'à ce qu'il réponde à une plainte client sur un ton que personne n'a approuvé, et personne ne s'en aperçoit pendant deux jours.

POINTS À VÉRIFIER

Qui est la personne responsable nommée de cet agent, et à quelle fréquence révise-t-elle ses résultats? Pouvez-vous expliquer, en langage clair, quelles décisions il peut prendre sans intervention humaine? S'il coordonne son action avec d'autres outils automatisés, leur activité combinée pourrait-elle paraître organisée ou intentionnelle aux yeux d'un observateur externe, même si personne ne l'a conçue ainsi?

MESURES À PRENDRE

Dressez l'inventaire de tout agent IA disposant d'une quelconque autonomie : ce qu'il peut faire sans approbation, qui en est responsable, et comment on s'apercevrait d'un problème. Intégrez un point de contrôle humain proportionnel à ce que l'agent peut réellement faire et consulter, y compris les modes de défaillance prévisibles, et non seulement ce pour quoi il a été conçu.

PRINCIPE

Un agent qui agit sans qu'un nom y soit rattaché demeure de votre responsabilité.

Adapté de l'avis n° 22 sur les normes d'éthique de la PRSA, « AI Agents in Public Relations ».

09

Liste de vérification pour bien démarrer

Que vous débutiez ou peaufiniez votre processus.

09 | LISTE DE VÉRIFICATION POUR BIEN DÉMARRER

Les Lignes directrices sur l'IA de la SCRP indiquent déjà comment bâtir l'infrastructure de base :

une liste d'outils approuvés,	un processus de révision et d'approbation,	une voie d'escalade, et	une politique de base sur l'utilisation de l'IA.

Si rien de tout cela n'existe encore, commencez par là. La demande est bien réelle : l'Atlas de la confiance envers l'IA 2026 de TELUS révèle que 59 % des Canadiens souhaitent en apprendre davantage sur l'IA. Voici cinq mesures concrètes pour vous aider à démarrer dans vos tâches quotidiennes de communications et de relations publiques.

☑	1. Évaluez vos résultats à l'aide d'une structure de risque. Utilisez les questions de la section 4 pour établir un niveau pour tout ce que l'IA touche.	SECTION 04
☑	2. Élaborez votre propre modèle de vérification. Partez de la chaîne de révision par niveaux et du cadre SAR de la section 4 plutôt que d'une page blanche. Adaptez-le à la charge de travail réelle de votre équipe.	SECTION 04
☑	3. Personne n'approuve son propre résultat d'IA à partir du niveau 2. La matrice de révision et d'approbation de la section 5 précise qui vérifie quoi. Maintenez cette séparation même au sein d'une petite équipe, où une personne peut assumer plus d'une vérification, mais jamais toutes sur le même dossier.	SECTION 05
☑	4. Divulguez votre utilisation et votre processus de vérification. Le test de confiance et le modèle de libellé de divulgation de la section 6 couvrent cet aspect. Incluez la vérification et la révision humaine dans votre divulgation.	SECTION 06
☑	5. Élaborez et testez un plan d'intervention en cas de crise pour l'IA. La voie d'escalade de la section 5 est le point de départ. Testez-le avant d'en avoir besoin : menez un exercice de simulation à l'aide de l'un des scénarios de la section 8.	SECTION 05/08

10

Ressources

Quelques études et réflexions à l'origine de cette trousse.

10 | RESSOURCES ET LIENS

Ces ressources ont servi à l'élaboration de la trousse. Elles sont énumérées selon leur ordre de première apparition dans le document.

N°	SOURCE	LIEN	ENDROIT
1	**Lignes directrices sur l'IA de la SCRP**	Approuvées par le conseil d'administration national de la SCRP, août 2026. https://www.cprs.ca/Advocacy/AIinPRPanel-(1)?lang=fr-CA	Section 1
2	**Étude de la SCRP sur l'état des relations publiques au Canada 2025**	SCRP, octobre 2025. cprs.ca (PDF)	Section 1
3	**BCG — GenAI Adoption in Corporate Affairs and Communications**	Boston Consulting Group, 2026. bcg.com	Section 1
4	**IPR — The Communicator's Role in Driving Generative AI Adoption**	Institute for Public Relations, février 2026. instituteforpr.org (PDF)	Section 1 (répété à la section 3)
5	**CIPR Inside — AI and Digital Ethics for Communicators**	CIPR Inside Committee, mai 2026. cipr.co.uk / newsroom.cipr.co.uk	Section 1 (guide source de cette trousse)
6	**Global Alliance for PR and Communication Management — Engagement de Venise / Principes pour une IA responsable**	globalalliancepr.org	Section 1
7	**CPVP — Principes pour une IA générative responsable, digne de confiance et respectueuse de la vie privée**	Commissariat à la protection de la vie privée du Canada.	Section 2
8	**CPVP — Conclusion en vertu de la LPRPDE n° 2026-002 (OpenAI)**	Commissariat à la protection de la vie privée du Canada. priv.gc.ca	Section 2

N°	SOURCE	LIEN	ENDROIT
9	**CPVP — Conclusion en vertu de la LPRPDE n° 2026-004 (X Corp / xAI, Grok)**	Commissariat à la protection de la vie privée du Canada, juin 2026. priv.gc.ca	Section 2 (répété à la section 3)
10	**Center for Countering Digital Hate — Grok floods X with sexualized images**	Center for Countering Digital Hate. counterhate.com	Section 2
11	**SCT — Guide sur l'utilisation de l'IA générative (principes FASTER)**	Secrétariat du Conseil du Trésor du Canada. canada.ca	Section 2 (répété à la section 3)
12	**SCT — Directive sur la prise de décisions automatisée**	Secrétariat du Conseil du Trésor du Canada. canada.ca	Section 2 (répété aux sections 3 et 9)
13	**Loi sur la protection des renseignements personnels dans le secteur privé (Québec, P-39.1 / Loi 25)**	RLRQ c P-39.1, à jour au 1er avril 2026. legisquebec.gouv.qc.ca	Sections 2, 4 et 6
14	**IBM Security / Ponemon — Cost of a Data Breach Report 2025: The AI Oversight Gap**	IBM Security / Ponemon Institute, 2025. ibm.com | https://canada.newsroom.ibm.com/2025-09-03-IBM-R-Study-Shadow-AI-Use-Surges-as-Canadian-Workers-Outpace-Employers-in-AI-Adoption	Section 2
15	**TELUS — Atlas de la confiance envers l'IA 2026**	TELUS, en partenariat avec Léger, janvier 2026. assets.ctfassets.net (PDF)	Sections 2, 3, 4, 6 (deux fois) et 9
16	**CRIC — Principes directeurs pour l'utilisation de l'IA en recherche marketing**	, les Principes directeurs pour l'utilisation de l'IA en recherche marketing du Conseil de recherche et d'intelligence marketing canadien (CRIC)	Sections 3, 4 et 5
17	**Dr Alex Sévigny — 4 leadership capabilities for communicators in the AI age**	alexsevigny.ca, juillet 2026. alexsevigny.ca	Section 3

N°	SOURCE	LIEN	ENDROIT
18	**Dr Alex Sévigny — Efficacy vs effectiveness vs efficiency in communications and marketing**	alexsevigny.ca, octobre 2025. alexsevigny.ca	Section 3
19	**Gerlich, M. (2025) — AI Tools in Society: Impacts on Cognitive Offloading and the Future of Critical Thinking**	https://doi.org/10.3390/soc15010006	Section 3
20	**Commission européenne — Code de bonnes pratiques sur le marquage et l'étiquetage des contenus générés par l'IA**	digital-strategy.ec.europa.eu	Section 5
21	**Schilke, O. and Reimann, M. (2025) — The transparency dilemma: How AI disclosure erodes trust**	Organizational Behavior and Human Decision Processes (OBHDP), 188, 104405. sciencedirect.com	Section 6
22	**Moffatt c. Air Canada**	2024 BCCRT 149 https://decisions.civilresolutionbc.ca/crt/crtd/en/item/525448/index.do?q=moffat	Section 8
23	**PRSA Board of Ethics and Professional Standards — Ethical Standard Advisory #22: AI Agents in Public Relations**	Août 2026 https://www.prsa.org/docs/default-source/about/ethics/esa-22.pdf?sfvrsn=867ef5c2_1	Section 8

CPRS | SCRP

Société canadienne des communications et des relations publiques | 2026

www.cprs.ca