COGNITIVE SECURITY
SÉCURITÉ COGNITIVE
CANADA

Perceive • Percevoir | Analyze • Analyser | Integrate • Intégrer

RAPPORT DE RECHERCHE

Microconformité

Le conditionnement stratifié du comportement humain dans les systèmes médiatisés par l'IA

Numéro du rapport	**COGSECCAN RR-003-FR**
Date de publication	Mai 2026
Préparé par	Sécurité Cognitive Canada
Classe d'information	Recherche d'intérêt public

Perceive / Percevoir • Analyze / Analyser • Integrate / Intégrer

Contrôle du document

Type de document	Rapport de recherche
Numéro du rapport	COGSECCAN RR-003-FR
Titre	Microconformité : le conditionnement stratifié du comportement humain dans les systèmes médiatisés par l'IA
Statut de publication	Diffusion publique
Préparé par	Sécurité Cognitive Canada
Version	v1.0-FR
Notes	Modèle de rapport de recherche

Résumé exécutif

La microconformité décrit le façonnement progressif du comportement humain par de petits actes répétés et peu frictionnels d'accord, de divulgation, d'attention, de conformité ou de réponse routinière. Il ne s'agit pas d'un grand acte d'obéissance. Il s'agit de l'accumulation d'actions ordinaires : cliquer sur accepter, suivre un parcours recommandé, laisser un paramètre par défaut inchangé, répondre à une alerte, accepter une petite divulgation, compléter une invite ou éviter un chemin de refus plus difficile. Avec le temps, ces petits actes peuvent entraîner les personnes à se comporter à l'intérieur de la logique d'un système sans se sentir directement contraintes.

Ce rapport soutient que la microconformité est un enjeu émergent de sécurité cognitive parce que les systèmes numériques et institutionnels modernes façonnent de plus en plus le jugement humain au moyen de paramètres par défaut, d'invites, de notifications, de ludification, de classements, de personnalisation algorithmique, de preuve sociale, de friction et d'exigences automatisées de flux de travail. Ces mécanismes opèrent souvent sous le seuil de résistance consciente. Ils ne retirent pas le choix au sens formel; ils modifient plutôt les choix qui semblent les plus faciles, rapides, sûrs, normaux ou les moins coûteux.

Le concept est plus large que les motifs trompeurs, les nudges, l'ingénierie sociale ou la propagande. Les motifs trompeurs désignent généralement des tactiques d'interface manipulatrices comme les options de refus cachées, les abonnements difficiles à annuler, les cases précochées ou le design visuel trompeur. Les nudges renvoient à l'utilisation de l'architecture du choix pour orienter les décisions tout en conservant des options formelles. L'ingénierie sociale exploite la confiance, l'urgence, l'émotion ou l'autorité pour produire une action nuisible. La propagande tente d'influencer les croyances et l'opinion à grande échelle. La microconformité relie ces champs en se concentrant sur le conditionnement comportemental répété de faible intensité dans la vie quotidienne, les milieux de travail, les services publics, les plateformes de consommation, les assistants d'IA et les environnements d'information civique.

La préoccupation centrale d'intérêt public est que la microconformité peut réduire l'autonomie significative tout en préservant l'apparence du consentement. En termes juridiques ou administratifs, l'utilisateur peut avoir cliqué, accepté, reconnu ou continué. En termes de sécurité cognitive, la question plus profonde est de savoir si la personne a eu une possibilité équitable de remarquer, comprendre, refuser, délibérer ou choisir autrement. Si l'environnement est conçu de sorte que le consentement soit plus facile que la compréhension et que la conformité soit plus facile que le refus, alors l'autonomie est affaiblie même lorsque le choix formel demeure disponible.

Ce rapport standardisé utilise un modèle de systèmes humains à six couches : la couche cognitive humaine, la couche de design d'interface, la couche algorithmique, la couche institutionnelle, la couche des acteurs de menace et la couche de gouvernance. Il introduit aussi la dérive de conformité : le mouvement graduel des individus, des organisations ou des communautés qui s'éloignent du jugement actif pour s'aligner automatiquement sur les signaux du système. La dérive de conformité explique comment des petits actes répétés peuvent normaliser un consentement faible, des décisions précipitées, des reconnaissances non lues, la dépendance algorithmique et une responsabilité fondée sur la complétion sans compréhension véritable.

Pour le Canada, la microconformité devrait être traitée comme un enjeu de gouvernance d'intérêt public. Les cadres existants en matière de vie privée, de protection du consommateur, d'accessibilité, de cybersécurité, de travail, de plateformes et de gouvernance de l'IA abordent chacun une partie du problème, mais aucun ne saisit pleinement le schéma commun : le façonnement du jugement humain par un conditionnement comportemental répété et peu frictionnel. Une réponse canadienne devrait combiner le respect de la vie privée par défaut, l'application des règles contre les motifs trompeurs, la transparence algorithmique, l'équité d'interface, la littératie numérique, l'audit indépendant, des services publics accessibles et une gouvernance avec intervention humaine.

Constat principal : Vous prenez peut-être encore des décisions, mais l'environnement peut décider quelles décisions semblent les plus faciles, rapides, sûres ou normales.

Carte du contenu

Définition et portée

La microconformité est l'alignement répété et peu frictionnel du comportement humain sur des signaux, des invites, des paramètres par défaut, des incitations, des pressions ou des attentes sociales conçus par un système. Il s'agit d'un schéma de petits ajustements comportementaux qui paraissent mineurs isolément, mais qui peuvent devenir importants lorsqu'ils se répètent dans le temps, sur plusieurs plateformes, institutions et contextes sociaux.

Le terme aide à décrire une condition croissante de la vie numérique. Les personnes sont constamment invitées à accepter, reconnaître, mettre à jour, confirmer, vérifier, partager, s'abonner, continuer, compléter, évaluer, commenter, approuver ou procéder. Chaque demande peut être défendable en soi. Un portail gouvernemental a besoin d'une vérification d'identité. Un milieu de travail a besoin d'une reconnaissance de politique. Une plateforme a besoin de paramètres de confidentialité. Une banque a besoin de contrôles antifraude. Le problème commence lorsque l'environnement total entraîne les personnes à traverser rapidement de petits actes de conformité sans attention significative.

La microconformité ne devrait pas être comprise comme l'affirmation que les personnes n'ont aucune agentivité. L'affirmation plus forte est que l'agentivité s'exerce à l'intérieur d'environnements structurés. Les interfaces, les paramètres par défaut, les procédures institutionnelles et les systèmes de recommandation personnalisés façonnent les conditions dans lesquelles les personnes exercent leur jugement. Ils influencent ce qui apparaît en premier, ce qui semble recommandé, ce qui exige un effort, ce qui paraît socialement normal et quelles conséquences sont attachées au refus.

Ce rapport inclut les interfaces numériques, les systèmes médiatisés par l'IA, les plateformes de consommation, les systèmes de travail, les portails de services publics, les contextes de cybersécurité et de fraude, ainsi que les environnements d'information civique. Il ne prétend pas que toute influence est nuisible, que la commodité est intrinsèquement manipulatrice ou que les utilisateurs sont impuissants. L'objet est plus précis : les situations où des schémas de design répétés et peu frictionnels affaiblissent la possibilité réelle de remarquer, comprendre, refuser, revenir en arrière ou exercer un jugement indépendant.

Tableau 1. La microconformité comparée à des concepts apparentés

Concept	Sens principal	Différence avec la microconformité
Nudge	Orientation des choix par l'architecture du choix tout en préservant des options formelles.	La microconformité se concentre sur le conditionnement comportemental répété dans le temps et entre les systèmes.
Motifs trompeurs	Design d'interface manipulateur qui oriente, obscurcit ou affaiblit le choix de l'utilisateur.	Les motifs trompeurs sont un mécanisme; la microconformité inclut aussi les milieux de travail, les services publics, les systèmes d'IA et les normes sociales.

Concept	Sens principal	Différence avec la microconformité
Ingénierie sociale	Manipulation du jugement humain par la confiance, l'urgence, la tromperie ou l'autorité.	La microconformité explique le sillon comportemental qui rend efficaces les demandes d'apparence routinière.
Propagande	Communication organisée visant à influencer l'opinion publique ou les croyances.	La microconformité agit au niveau des petites actions, souvent avant la formation complète des croyances.
Conformité	Suivre des instructions, des règles ou des attentes.	La microconformité est souvent habituelle, pré-réflexive, peu frictionnelle et induite par le système.
Design comportemental	Concevoir des environnements pour influencer l'action.	La microconformité demande à quel moment le design devient une érosion de l'autonomie.

Questions de recherche et méthode

Questions de recherche

No	Question directrice
1	Qu'est-ce que la microconformité, et comment peut-elle être distinguée de la conformité ordinaire, des nudges, des motifs trompeurs, de la propagande et de l'ingénierie sociale?
2	Comment les environnements numériques, institutionnels et médiatisés par l'IA façonnent-ils l'attention, le consentement, la prise de décision et l'autonomie comportementale par des actions répétées et peu frictionnelles?
3	Quels risques d'intérêt public apparaissent lorsque de petits actes répétés d'accord sont traités comme preuve d'un consentement valide, d'une compréhension ou d'une responsabilité?
4	Comment les cadres de gouvernance canadiens devraient-ils traiter la microconformité dans les domaines de la vie privée, de la protection du consommateur, de la cybersécurité, de l'accessibilité, du travail, du design des services publics et de la gouvernance de l'IA?
5	Quelles garanties pratiques peuvent préserver le choix significatif, le refus, la réversibilité et le jugement humain dans les systèmes à forte friction ou à fort impact?

Méthode et base documentaire

Ce rapport utilise une synthèse analytique plutôt qu'une recherche empirique primaire. Il intègre des concepts issus de l'économie comportementale, de la recherche sur les motifs trompeurs, des orientations en matière de vie privée et de protection du consommateur, de la sensibilisation à la cybersécurité, de la littérature sur l'ingénierie sociale, du design des services publics et des discussions émergentes sur la gouvernance de l'IA.

La base documentaire comprend des documents réglementaires publics d'organismes canadiens et internationaux, des concepts universitaires sur l'architecture du choix et la conformité incrémentale, des analyses juridiques et politiques sur le design trompeur, ainsi que des explications de cybersécurité sur la manipulation ciblant l'humain. Le rapport traite la

microconformité comme un cadre interprétatif d'intérêt public plutôt que comme un terme juridique établi.

L'analyse évite les affirmations causales non appuyées. Elle n'affirme pas qu'une plateforme ou un système donné a directement causé un résultat psychologique précis sans preuve disponible. Elle identifie plutôt des mécanismes observables, des lacunes de gouvernance et des questions pratiques pour la recherche future.

Limites et incertitude

Limite / point d'incertitude	Implication pour l'analyse
Concept émergent	La microconformité est un concept émergent qui exige une validation empirique supplémentaire.
Distinctions contextuelles	Le consentement, la manipulation, la persuasion, la commodité et les nudges légitimes d'intérêt public doivent être distingués avec soin selon le contexte.
Lecture prudente des taux de conformité	Des taux élevés de conformité peuvent indiquer une préférence des utilisateurs, mais ils peuvent aussi indiquer une asymétrie de friction ou une pression de design; un audit indépendant est nécessaire pour faire la distinction.
Évolution rapide de l'IA	L'influence médiatisée par l'IA évolue rapidement; les recherches futures devraient donc réviser la terminologie, les voies réglementaires et les normes de preuve à mesure que les systèmes évoluent.

Cadre conceptuel

La sécurité cognitive s'intéresse aux conditions dans lesquelles les individus et les communautés perçoivent, interprètent, décident et agissent. La microconformité est pertinente parce qu'elle cible l'environnement pré-décisionnel : les signaux, les invites, les paramètres par défaut, les pressions et les indices sociaux qui façonnent le comportement avant qu'une personne ne réfléchisse pleinement.

Les cadres de sécurité traditionnels séparent souvent les vulnérabilités techniques du comportement humain. La cybersécurité traite l'hameçonnage comme une attaque ciblant l'humain. Le droit de la vie privée traite le consentement comme un problème d'information et de contrôle. Le droit de la consommation traite le design trompeur comme une pratique de marché déloyale. La politique du travail traite les tableaux de bord numériques et les systèmes automatisés de performance comme des enjeux de milieu de travail. La gouvernance de l'IA traite les recommandations automatisées et les systèmes d'aide à la décision comme des enjeux de responsabilité algorithmique. La microconformité traverse ces champs parce que l'enjeu commun est le façonnement répété du jugement humain par des signaux peu frictionnels.

Une lentille de sécurité cognitive demande si une personne pouvait réellement remarquer l'influence, comprendre le choix, comparer les alternatives, refuser sans pénalité et revenir sur la décision plus tard. Une bannière de consentement peut techniquement présenter des options, tout en biaisant l'utilisateur si le chemin d'acceptation est lumineux, immédiat et simple alors que le refus est caché, retardé ou formulé avec culpabilisation. Une plateforme de formation en

milieu de travail peut techniquement enregistrer une reconnaissance, mais échouer malgré tout si les employés cliquent sans comprendre parce que la complétion est récompensée davantage que le jugement.

La question n'est pas de savoir si toute influence est mauvaise. Les sociétés humaines reposent sur la persuasion légitime, les rappels, l'orientation, la formation et les nudges d'intérêt public. La question est de savoir si l'influence demeure transparente, proportionnée, réversible, contestable et alignée avec les intérêts de l'utilisateur. La microconformité devient nuisible lorsque l'objectif du système remplace la capacité de la personne de comprendre ou de refuser.

Modèle de systèmes humains à six couches

Couche	Mécanisme	Indicateurs courants
Cognitive humaine	Fatigue, surcharge, urgence, ambiguïté, pression sociale.	Clics rapides, acceptation des valeurs par défaut, lecture réduite, évitement de l'option plus difficile.
Design d'interface	Hiérarchie visuelle, asymétrie des boutons, refus caché, continuité forcée.	Chemin d'acceptation plus facile que le chemin de refus; annulation ou suppression difficile à trouver.
Algorithmique	Classement personnalisé, recommandations, notifications, boucles de rétroaction.	Invites adaptées répétées; dépendance accrue aux parcours recommandés.
Institutionnelle	Formulaires, tableaux de bord, reconnaissances, modules obligatoires, nudges de flux de travail.	La complétion est mesurée plus que la compréhension; clics routiniers de reconnaissance de politiques.
Acteur de menace	Imitation d'invites légitimes et de signaux d'autorité.	Hameçonnage, fraude, fausse vérification, recrutement incrémental, couloirs de désinformation.
Gouvernance	Lois, normes, audits, accessibilité, responsabilité.	Présence ou absence de consentement significatif, de transparence, de refus facile et de recours.

Dérive de conformité

La dérive de conformité est le mouvement graduel d'une personne, d'un groupe ou d'une institution qui s'éloigne du jugement actif pour s'aligner automatiquement sur les signaux du système. Elle apparaît lorsque de petits actes répétés d'accord routinier se normalisent. L'utilisateur cesse de lire les avis de consentement. L'employé signe des reconnaissances sans compréhension. Le citoyen suit les instructions d'un portail sans comprendre ses droits ou les alternatives. L'organisation mesure la complétion plutôt que la compréhension.

La dérive de conformité est importante parce qu'elle convertit le comportement en preuve. Un module complété devient une preuve de formation. Une case cochée devient une preuve de consentement. Un accusé de réception cliqué devient une preuve de connaissance. Pourtant, la réalité cognitive peut être différente : la personne a peut-être agi sous pression, fatigue,

confusion, asymétrie d'interface ou attente sociale. L'apparence de responsabilité peut exister sans jugement véritable.

Données probantes et études de cas

Contexte	Mécanisme observable	Pourquoi cela compte
Vie numérique quotidienne	Une personne se réveille et consulte son téléphone avant de former un plan délibéré pour la journée. Les notifications, les mises à jour d'applications, les bannières, les messages et l'information ordonnée par algorithme entraînent l'attention à répondre plutôt qu'à réfléchir.	L'attention est orientée avant que l'intention soit pleinement formée.
Plateformes de consommation	Les sites de commerce en ligne peuvent utiliser des signaux de rareté, des comptes à rebours, des ajouts recommandés, des achats en un clic, des renouvellements automatiques, des options présélectionnées et des abonnements difficiles à annuler.	L'achat est façonné par une séquence de petites décisions de conformité.
Bannières de témoins et consentement à la vie privée	Les interfaces de consentement aux témoins de connexion présentent souvent un chemin d'acceptation rapide et un chemin de refus plus lent.	Le consentement n'est significatif que lorsque l'utilisateur peut comprendre le choix et refuser sans friction indue.
Systèmes de travail	Les employés peuvent recevoir des invites répétées pour compléter des formations, reconnaître des politiques, mettre à jour des tableaux de bord, répondre à des outils de collaboration et suivre des nudges de flux de travail.	La vitesse et la complétion peuvent être récompensées davantage que la compréhension.
Systèmes publics et accès civique	Les portails gouvernementaux peuvent améliorer l'efficacité, mais la prestation numérique des services peut aussi exclure les personnes confrontées à une faible littératie numérique, à des barrières linguistiques, à des handicaps, à des traumatismes, à la pauvreté ou à un accès limité à la technologie.	La participation peut devenir une épreuve de capacité à la microconformité.
Assistants d'IA et aide à la décision	Les outils d'IA peuvent intensifier la microconformité parce qu'ils fournissent des suggestions fluides, confiantes et peu frictionnelles.	Les utilisateurs peuvent être conditionnés à accepter un cadrage généré par la machine avant de former le leur.
Médias sociaux et systèmes de recommandation	Les fils algorithmiques convertissent les clics, pauses, visionnements, mentions J'aime, partages, commentaires et recherches en rétroaction pour le classement futur.	Les parcours recommandés peuvent devenir à la fois environnement et habitude.

Indicateurs de mesure

Indicateur	Ce qu'il peut révéler
Différentiel de taux de consentement	Si l'acceptation change fortement lorsque les options accepter et refuser sont également visibles.

Indicateur	Ce qu'il peut révéler
Friction du refus	Le nombre d'étapes, d'écrans, d'invites émotionnelles ou de délais nécessaires pour refuser.
Difficulté de réversibilité	Si l'utilisateur peut facilement annuler un consentement, annuler un abonnement, supprimer des données ou modifier des paramètres.
Score de compréhension	Si la personne a compris ce qu'elle a accepté, et non seulement si elle a cliqué.
Charge d'accessibilité	Si le système impose un effort disproportionné aux personnes handicapées, aux personnes ayant des barrières linguistiques, une faible littératie numérique ou un accès limité.
Fréquence des notifications	Si l'attention est interrompue de façon répétée avant que le jugement intentionnel puisse se former.
Prévalence des motifs trompeurs	Si des schémas d'interface trompeurs ou obstructifs apparaissent dans un service ou un secteur.

Analyse des menaces et des risques

Situation de risque	Lecture opérationnelle
Imitation des routines légitimes	Les attaques d'hameçonnage reproduisent souvent le langage et la logique visuelle des systèmes légitimes : compte nécessitant une action, vérification immédiate, code à scanner, connexion à approuver, paiement à mettre à jour ou identité à confirmer.
Fraude incrémentale	Une victime peut commencer par une action mineure, puis passer à des demandes croissantes. Chaque étape réduit la résistance à la suivante.
Recrutement et désinformation	Regarder, aimer, partager, rejoindre, commenter ou participer peut renforcer l'identité, l'engagement et l'exposition algorithmique.
Milieux de travail	Tableaux de bord, classements, nudges automatisés et invites constantes peuvent entraîner l'autocensure, l'accélération, la surdivulgation ou l'acceptation routinière de la surveillance.
Urgences et panique publique	En situation de crise, les habitudes de microconformité peuvent accélérer la désinformation, la fraude, les achats de panique ou les comportements dangereux.

Résumé des schémas de risque

Schéma de risque	Préoccupation d'intérêt public	Orientation de sauvegarde
Consentement faible	L'accord est enregistré sans compréhension significative.	Chemins de refus équivalents, explication en langage clair, réversibilité facile.
Compression du jugement	Les personnes sont poussées à agir rapidement plutôt qu'à réfléchir.	Moins d'invites, contrôles de compréhension, pauses pour les décisions à fort impact.

Schéma de risque	Préoccupation d'intérêt public	Orientation de sauvegarde
Imitation par acteurs de menace	Les attaquants copient les routines légitimes d'invite.	Redessiner les systèmes légitimes pour réduire les clics réflexes et les habitudes de vérification urgente.
Exclusion par accessibilité	La friction numérique bloque l'accès aux services ou aux droits.	Soutien humain, alternatives non numériques, tests d'accessibilité.
Dépendance algorithmique	Les utilisateurs adoptent le cadrage du système avant l'interprétation indépendante.	Recommandations transparentes, contrôles de personnalisation, examen avec intervention humaine.

Gouvernance et droit

Le Canada dispose de plusieurs voies de gouvernance pertinentes, mais elles sont fragmentées. Le droit de la vie privée traite le consentement et les renseignements personnels. La protection du consommateur traite les pratiques commerciales trompeuses. Le droit de la concurrence traite les déclarations trompeuses et les conduites de marché. Les cadres d'accessibilité traitent l'utilisabilité et l'inclusion. Le droit du travail traite les conditions de travail et la surveillance. La cybersécurité traite l'hameçonnage et les attaques ciblant l'humain. La gouvernance de l'IA traite les systèmes automatisés et la responsabilité. La microconformité exige une coordination entre ces domaines.

Les organismes publics canadiens reconnaissent déjà les motifs trompeurs comme un problème. L'Office de la consommation d'Innovation, Sciences et Développement économique Canada décrit les motifs trompeurs comme des designs web ou applicatifs qui peuvent influencer la prise de décision et amener les utilisateurs à céder du temps, de l'argent, de la vie privée ou des renseignements personnels. Le balayage de 2024 du Commissariat à la protection de la vie privée du Canada a examiné les motifs de design trompeur et signalé des indicateurs dans presque tous les sites web et applications testés. Ces constats soutiennent une préoccupation plus large de sécurité cognitive : le design manipulateur d'interface n'est pas rare; il fait partie de l'environnement numérique ordinaire.

La gouvernance de l'IA devrait traiter non seulement les décisions automatisées biaisées ou nuisibles, mais aussi l'influence automatisée : recommandations, classement, invites personnalisées, suggestions agentiques et flux de consentement médiatisés par l'IA. À mesure que les assistants d'IA deviennent conversationnels et adaptatifs, les préoccupations de sécurité cognitive se déplacent des boutons visibles vers le cadrage fluide, l'autorité implicite et la délégation peu frictionnelle.

Les services publics méritent une attention particulière. Les citoyens n'ont pas toujours d'alternative réaliste aux portails gouvernementaux. Cela crée un devoir plus élevé d'assurer l'équité, l'accessibilité, le langage clair, la réversibilité facile, le soutien humain significatif et des chemins de refus non punitifs. Le gouvernement numérique ne devrait pas transformer l'accès administratif en test de capacité à la microconformité.

Carte des lacunes de gouvernance

Domaine	Objet actuel	Lacune de microconformité
Vie privée	Consentement et renseignements personnels.	Le consentement peut être techniquement enregistré alors que le design d'interface affaiblit la compréhension réelle ou le refus.
Protection du consommateur	Pratiques de marché fausses, trompeuses, déloyales ou mensongères.	La friction subtile et le conditionnement comportemental peuvent ne pas être traités comme un enjeu central d'autonomie.
Cybersécurité	Hameçonnage, fraude, attaques ciblant l'humain.	La formation peut blâmer les utilisateurs sans traiter les systèmes qui conditionnent les clics réflexes.
Accessibilité	Accès inclusif et utilisabilité.	La friction des services numériques peut devenir une exclusion lorsque la capacité de microconformité est présumée.
Travail et milieu de travail	Conditions d'emploi, surveillance, outils de performance.	Les tableaux de bord et les invites peuvent comprimer le jugement et normaliser la surconformité.
Gouvernance de l'IA	Décisions automatisées, transparence, gestion des risques.	L'influence automatisée, les invites de recommandation et le consentement médiatisé par l'IA doivent être explicitement traités.

Recommandations pour le Canada

Les recommandations ci-dessous standardisent le plan d'action original de RR-002 dans le format du rapport de recherche maître. Les priorités devraient commencer par la sensibilisation, l'orientation et l'audit, puis évoluer vers des normes applicables dans les contextes à haut risque.

Recommandation	Acteurs principaux	Échéancier	Complexité
Développer un axe canadien de recherche sur la microconformité avec des études de cas, des notes publiques et des analyses sectorielles.	COGSEC Canada, universités, société civile	Court terme	Faible à moyenne
Renforcer l'application contre le design trompeur et clarifier que le design manipulateur ou obstructif peut affaiblir le consentement significatif.	CPVP, Bureau de la concurrence, organismes de consommation	Court terme	Moyenne

Recommandation	Acteurs principaux	Échéancier	Complexité
Créer des normes d'équité d'interface pour l'égale visibilité des options accepter/refuser, la réversibilité facile, le langage clair, le design accessible et la divulgation de la personnalisation.	CSA, régulateurs, associations UX	Moyen terme	Moyenne
Exiger des évaluations d'impact d'influence pour les systèmes numériques à fort impact, y compris les assistants d'IA, les systèmes de recommandation, les portails de services publics, les plateformes de surveillance des employés et les systèmes intensifs en consentement.	Décideurs fédéraux et provinciaux	Moyen terme	Élevée
Auditer les services numériques publics pour la charge d'accessibilité, la friction du refus, la qualité du consentement et l'exclusion causée par la friction numérique.	Conseil du Trésor, provinces, municipalités	Moyen terme	Moyenne
Intégrer la microconformité à la prévention de l'hameçonnage, de la fraude et de l'ingénierie sociale en passant du blâme des utilisateurs à la refonte des systèmes.	Agences de cybersécurité, employeurs, écoles	Court terme	Faible
Établir une surveillance indépendante des motifs trompeurs des plateformes, des systèmes de recommandation, des flux de consentement, des chemins d'annulation et des barrières d'accès numérique aux services publics.	Régulateurs, chercheurs, société civile	Long terme	Élevée

Calendrier de mise en œuvre

Phase	Horizon temporel	Objectif de mise en œuvre	Résultats représentatifs

Phase	Horizon temporel	Objectif de mise en œuvre	Résultats représentatifs
Phase 1 : Sensibilisation et recherche de base	Court terme	Définir la microconformité pour les publics canadiens; documenter des études de cas; intégrer les concepts aux ressources de cybersécurité, de vie privée et de littératie numérique.	Note publique, glossaire, première série d'études de cas, insertion de formation.
Phase 2 : Orientation et normes	Moyen terme	Développer des normes d'équité d'interface, des critères de facilité du refus, des vérifications d'accessibilité et des orientations sur la qualité du consentement pour les systèmes publics et privés.	Notes d'orientation, liste d'audit, modèle d'écran de consentement, langage de passation de marchés.
Phase 3 : Audits institutionnels	Moyen terme	Examiner les portails publics, les plateformes de travail, les systèmes scolaires et les services numériques à fort impact pour la charge de microconformité.	Rapports d'audit, plans de correction, refonte en langage clair.
Phase 4 : Gouvernance applicable	Long terme	Passer des orientations volontaires à des attentes applicables dans les contextes à risque élevé; bâtir une capacité de surveillance indépendante.	Normes réglementaires, exigences d'audit, mécanismes de recours, rapport annuel de surveillance.
Phase 5 : Garanties pour l'influence médiatisée par l'IA	Long terme	Adapter la gouvernance aux agents conversationnels, aux invites adaptatives, aux systèmes de recommandation et aux outils automatisés d'aide à la décision.	Évaluations d'impact d'influence, normes de divulgation pour assistants d'IA, garde-fous avec intervention humaine.

La mise en œuvre devrait demeurer proportionnée. Les fonctions de commodité à faible risque ne devraient pas être sur-réglementées, mais les systèmes à fort impact qui touchent les droits, l'accès, l'emploi, la vie privée, la sécurité ou la participation publique devraient être tenus de préserver un avis significatif, le refus, la réversibilité et le jugement humain.

Lacunes de recherche et prochaines étapes

La microconformité demeure sous-théorisée. Il faut davantage de recherche pour mesurer les effets cumulatifs dans le temps, identifier les populations vulnérables, comparer les risques propres aux secteurs et distinguer les nudges légitimes d'intérêt public du conditionnement manipulateur. La recherche devrait aussi examiner comment les assistants d'IA modifient le consentement, la confiance et la délégation décisionnelle.

Les recherches futures devraient inclure des entrevues qualitatives, des audits d'interface, des expériences contrôlées, des tests d'accessibilité des services publics, des études de cas en milieu de travail et des enquêtes longitudinales. Elles devraient aussi examiner la relation entre la microconformité, la liberté cognitive, l'ingénierie sociale, la désinformation et l'aide à la décision médiatisée par l'IA.

Sécurité Cognitive Canada peut contribuer en créant un observatoire de la microconformité : un axe de recherche d'intérêt public qui documente les schémas, publie des études de cas, crée des outils de sensibilisation et soutient le dialogue politique. L'observatoire pourrait suivre le design trompeur, la personnalisation algorithmique, les systèmes de conformité en milieu de travail, les services publics numériques et l'imitation des invites légitimes par les acteurs de menace.

Questions de recherche prioritaires

No	Question prioritaire
1	Comment la microconformité cumulative peut-elle être mesurée sur les plateformes, dans les milieux de travail et dans les services publics?
2	Quelles populations subissent une charge disproportionnée de microconformité en raison du handicap, de la langue, du traumatisme, de l'âge, du revenu ou de l'accès numérique limité?
3	Qu'est-ce qui distingue un nudge acceptable d'intérêt public d'un conditionnement manipulateur?
4	Comment les assistants d'IA modifient-ils la confiance, la délégation, le consentement et l'interprétation indépendante?
5	Quelles normes d’interface préservent le plus efficacement le refus et la réversibilité significatifs sans créer de friction inutile dans les services?

Conclusion

La microconformité ne concerne pas seulement les personnes qui cliquent sur des boutons. Elle concerne la manière dont les systèmes modernes entraînent discrètement les conditions dans lesquelles les personnes remarquent, décident, acceptent, refusent et se conforment. Elle décrit un déplacement de l'instruction explicite vers le façonnement environnemental, de la coercition ouverte vers l'asymétrie de friction, et du consentement éclairé vers l'accord routinisé.

Le concept est important parce qu'il révèle comment l'autonomie peut être affaiblie alors que le choix formel demeure intact. Une personne peut cliquer sur accepter, compléter un module, suivre une recommandation ou continuer dans un flux de travail, tout en ayant été guidée par la fatigue, l'urgence, un refus caché, la pression sociale ou la personnalisation algorithmique. La question centrale est de savoir si la personne a eu une chance significative de comprendre et de choisir autrement.

Pour le Canada, la microconformité offre un pont utile entre la sécurité cognitive, la vie privée, la protection du consommateur, la cybersécurité, la gouvernance de l'IA, les droits en milieu de travail, l'accessibilité et la résilience démocratique. Protéger l'autonomie cognitive exige plus

que combattre la désinformation. Il faut concevoir des systèmes qui préservent le jugement dans les petits moments.

La leçon publique est simple : vous prenez peut-être encore des décisions, mais l'environnement peut décider quelles décisions semblent les plus faciles, les plus rapides, les plus sûres ou les plus normales. La sécurité cognitive commence lorsque les personnes, les institutions et les décideurs apprennent à voir clairement cet environnement.

Références

Commissariat à la protection de la vie privée du Canada. (2024). Sweep Report 2024: Deceptive Design Patterns. Disponible à : https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-networks/international-privacy-sweep/2024_sweep/opc-sweep-report-2024/

Innovation, Sciences et Développement économique Canada, Office de la consommation. Dark patterns. Disponible à : https://ised-isde.canada.ca/site/office-consumer-affairs/en/dark-patterns

Federal Trade Commission. (2022). Bringing Dark Patterns to Light. Disponible à : https://www.ftc.gov/reports/bringing-dark-patterns-light

European Data Protection Board. (2022). Guidelines on Dark Patterns in Social Media Platform Interfaces. Disponible à : https://www.edpb.europa.eu/

Thaler, R. H., et Sunstein, C. R. (2008/2021). Nudge.

Cialdini, R. B. (2009). Influence: Science and Practice.

Freedman, J. L., et Fraser, S. C. (1966). Compliance without pressure: The foot-in-the-door technique. Journal of Personality and Social Psychology, 4(2), 195-202. https://doi.org/10.1037/h0023552

Johnson, E. J., et Goldstein, D. (2003). Do Defaults Save Lives? Disponible à : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1324774

Innovation, Sciences et Développement économique Canada. Artificial Intelligence and Data Act companion materials. Disponible à : https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

Association du Barreau canadien. Privacy Dark Patterns: A Case for Regulatory Reform in Canada. Disponible à : https://www.cba.org/sections/privacy-and-access/resources/privacy-dark-patterns-a-case-for-regulatory-reform-in-canada/

Proofpoint. What Is Social Engineering? Disponible à : https://www.proofpoint.com/us/threat-reference/social-engineering

Harvard Kennedy School. Short-term exposure to filter-bubble recommendation systems has limited polarization effects. Disponible à : https://www.hks.harvard.edu/publications/short-term-exposure-filter-bubble-recommendation-systems-has-limited-polarization

Citation suggérée

Sécurité Cognitive Canada. (2026). Microconformité : le conditionnement stratifié du comportement humain dans les systèmes médiatisés par l'IA. Rapport de recherche COGSECCAN RR-002-FR.

Avis de non-responsabilité

Ce rapport est destiné à la recherche d'intérêt public et à l'éducation. Il ne constitue pas un avis juridique, médical, de cybersécurité, financier, d'accessibilité, d'approvisionnement ou professionnel. Les constats reposent sur des sources publiques citées et une synthèse analytique au moment de la publication. Les affirmations devraient être vérifiées par rapport aux sources citées avant toute reliance institutionnelle formelle ou republication.