Cognitive Liberty in Canada: Protecting Mental Autonomy in the Digital Age

Version francaise - COGSECCAN_RR_001 - 05-02-2026

Avis: Ce document est une traduction francaise de travail preparee pour la publication bilingue sur le site de Cognitive Security Canada. Il est fourni a des fins de sensibilisation publique, de recherche et de discussion. Il ne constitue pas un avis juridique, medical, psychologique, d'enquete ou de securite.

Resume executif

Le droit canadien ne protege pas encore explicitement la "liberte cognitive", c'est-a-dire la capacite d'une personne de penser, de decider et de traiter l'information sans coercition, manipulation cachee ou influence indue. La Charte canadienne mentionne la liberte de pensee, de croyance, d'opinion et d'expression, mais la jurisprudence a surtout developpe ce droit autour de l'expression publique. De meme, la securite de la personne a ete interpretee comme incluant l'integrite psychologique, mais dans des contextes de prejudice grave et d'action etatique directe.

Ces doctrines ont ete developpees avant l'apparition des recommandations algorithmiques, de la publicite comportementale, des interfaces persuasives, des profils psychographiques et des systemes d'IA capables d'adapter continuellement l'environnement informationnel d'une personne. Les plateformes privees peuvent faconner ce que les gens voient, ressentent, croient ou evitent, souvent sans que l'utilisateur comprenne la logique de personnalisation.

Constats principaux

- Lacunes constitutionnelles: la Charte s'applique principalement a l'Etat, non aux plateformes privees. La liberte de pensee demeure peu developpee comme droit autonome protegeant l'espace mental.
- Lacunes civiles: le contrat, la responsabilite civile, l'influence indue et le consentement n'ont pas encore ete adaptes aux formes diffuses de persuasion algorithmique et de design manipulateur.
- Lacunes en protection de la vie privee: les lois sur les renseignements personnels encadrent surtout la collecte, l'utilisation et la communication de donnees, mais beaucoup moins l'usage de ces donnees pour influencer les croyances, l'attention ou les decisions.
- Tendances internationales: plusieurs chercheurs, commissions et organismes de droits humains discutent de neurodroits, de vie privee mentale, de liberte de pensee et d'integrite cognitive dans les environnements numeriques.
- Defis de preuve: demontrer une atteinte cognitive exige souvent des traces numeriques, des journaux de contenu, des analyses comportementales, des expertises psychologiques et des audits algorithmiques.

Recommandations

- Reconnaissance statutaire de la liberte cognitive ou de l'integrite cognitive comme valeur juridique fondamentale.
- Obligations de diligence pour les plateformes numeriques, les annonceurs et les fournisseurs de systemes d'IA lorsque leurs outils peuvent influencer les decisions humaines.
- Transparence algorithmique et controle utilisateur: explications claires, options de desactivation, portabilite des donnees de profil et etiquettes d'influence.
- Mandats explicites pour les organismes de protection de la vie privee, de concurrence et de consommation afin d'examiner les dommages cognitifs.
- Protocoles de preuve pour documenter l'influence: captures, chronologies, donnees de ciblage, audits, evaluations expertes et conservation securisee des elements.

1. Fondements juridiques de l'autonomie cognitive

Le point de depart canadien est la Charte. L'article 2(b) garantit la liberte de pensee, de croyance, d'opinion et d'expression. En pratique, les tribunaux ont surtout traite cette garantie comme une protection de l'expression. La dimension interieure - l'espace mental, la capacite de former une opinion ou la protection contre la manipulation cognitive - reste largement non developpee.

L'article 7 protege la vie, la liberte et la securite de la personne. La Cour supreme a reconnu que la securite de la personne peut inclure l'integrite psychologique lorsque l'Etat impose un prejudice grave et profond. Toutefois, cette protection demeure difficile a appliquer aux environnements numeriques prives, ou l'influence est cumulative, personnalisee, indirecte et souvent invisible.

Le droit des contrats suppose que les parties consentent librement. Les doctrines d'incapacite, de fausse representation, d'iniquite contractuelle ou d'influence indue existent, mais elles sont generalement construites autour de situations identifiables: relation de confiance, tromperie manifeste, transaction suspecte ou vulnerabilite exploitee. Elles ne repondent pas clairement a la question suivante: un consentement obtenu dans une architecture de choix opaque et manipulative est-il encore pleinement volontaire?

La responsabilite civile peut reparer certains dommages psychologiques, mais elle exige habituellement un prejudice identifiable, une faute, un lien causal et une proximite suffisante. Les systemes d'engagement numerique peuvent produire des effets diffus: anxiete, dependance, polarisation, perte d'attention, decisions impulsives ou retrait social. Ces effets sont difficiles a relier a une seule action fautive.

Domaine	Interet protege	Limite principale pour l'influence numerique
Charte art. 2(b)	Pensee, croyance, opinion, expression	Peu developpe comme protection de l'espace mental; vise surtout l'action etatique.
Charte art. 7	Vie, liberte, securite et integrite psychologique	Seuil eleve de prejudice grave; difficile pour les influences privees diffuses.
Contrats	Consentement, capacite, absence d'influence indue	Peu adapte aux interfaces persuasives et a la personnalisation algorithmique.
Responsabilite civile	Prevention et reparation de dommages previsibles	Causalite et proximite difficiles dans les systemes d'influence a grande echelle.
Vie privee et consommation	Donnees, consentement, marketing loyal	Encadre surtout la collecte et les fausses representations, pas la manipulation subtile.

2. L'influence dans l'environnement numerique

Les systemes modernes d'influence fonctionnent par couches. L'utilisateur voit un fil d'actualite, une recommandation, une notification, un bouton, une option par defaut ou une annonce. Derriere cette interface, des modeles determinent ce qui apparait, dans quel ordre, a quel moment, avec quelle repetition et selon quelles probabilites d'engagement.

- Systemes de recommandation: ils profilent les comportements et proposent des contenus afin de maximiser des mesures comme le temps passe, les clics ou les reactions.
- Publicite ciblee et influence politique: les donnees comportementales peuvent servir a adapter les messages aux vulnerabilites, preferences ou emotions supposees.
- Dark patterns et design manipulateur: certains parcours rendent l'acceptation facile et le refus couteux, confus ou cache.
- Desinformation et manipulation de contenu: des campagnes coordonnees peuvent exploiter l'incertitude, la peur, l'identite ou la colere.

- Design persuasif dans les applications: notifications, recompenses variables, boucles sociales et micro-incitations peuvent entrainer une adaptation continue.

L'enjeu n'est pas que toute influence soit illegitime. L'education, la persuasion honnete, la culture et le debat public reposent aussi sur l'influence. Le probleme survient lorsque l'influence devient cachee, asymetrique, personnalisee, coercitive ou concue pour contourner la reflexion.

3. Approches comparatives et tendances emergentes

A l'echelle internationale, le droit commence a reconnaitre que la liberte de pensee et l'integrite mentale doivent etre relues a la lumiere des technologies numeriques et des neurotechnologies. Le Royaume-Uni a integre, dans le contexte de la securite en ligne, une reference a la protection de la liberte de pensee et de conscience. L'Union europeenne traite deja certaines categories de donnees sensibles avec une protection accrue et encadre progressivement les systemes d'IA a haut risque. L'Australie a publie des analyses sur les neurotechnologies, l'IA et les limites traditionnelles de la pensee humaine.

Le Canada peut participer a cette evolution en developpant une approche prudente, non sensationnaliste et fondee sur des preuves. La question n'est pas de pretendre que toute interaction numerique est coercitive. Il s'agit plutot d'identifier les contextes ou la personnalisation, la surveillance commerciale, les incitations comportementales et l'opacite technique peuvent compromettre l'autonomie mentale.

4. Lacunes juridiques identifiees

- La Charte ne fournit pas de recours direct contre les acteurs prives qui structurent l'environnement informationnel quotidien.
- Le contrat presume un choix volontaire meme lorsque les interfaces reduisent la comprehension, augmentent la fatigue ou rendent le refus peu realiste.
- La responsabilite civile n'a pas encore etabli un devoir general de securite cognitive pour les plateformes.
- La vie privee protege les donnees, mais ne traite pas toujours l'influence rendue possible par ces donnees.
- Le droit de la concurrence et de la consommation cible les mensonges et certaines pratiques deloyales, mais pas necessairement la persuasion psychologique subtile.

Mecanisme d'influence	Probleme juridique	Question de reforme
Personnalisation algorithmique	Opacite et asymetrie informationnelle	Faut-il imposer des audits et explications?
Profilage psychologique	Consentement insuffisant ou trop general	Les profils mentaux devraient-ils etre des donnees sensibles?
Dark patterns	Choix oriente sans mensonge explicite	Devrait-on presumer une influence indue dans certains designs?
Campagnes de desinformation	Effets collectifs et diffus	Quels outils de transparence et de preuve sont necessaires?
IA persuasive	Automatisation de la persuasion a grande echelle	Quel devoir de diligence pour les deployeurs?

5. Reformes juridiques recommandees

5.1 Definir et reconnaitre les droits cognitifs

Une loi pourrait reconnaitre explicitement le droit de toute personne a l'integrite cognitive: l'autonomie de penser, croire, douter, interpreter et decider sans manipulation technologique non consentie. Une telle reconnaissance n'exigerait pas necessairement une modification constitutionnelle; elle pourrait apparaitre dans une loi sur la vie privee, l'IA, les droits de la personne ou la protection du consommateur.

5.2 Traiter les donnees mentales et les profils psychologiques comme sensibles

Les donnees qui revelent ou inferent des etats mentaux, des vulnerabilites, des croyances, des traits psychologiques ou des tendances comportementales devraient recevoir une protection accrue. Leur utilisation pour influencer des decisions devrait exiger un consentement clair, specifique et revocable.

5.3 Imposer un devoir de diligence aux plateformes

Les fournisseurs de plateformes, moteurs de recherche, reseaux sociaux et systemes d'IA a forte portee devraient evaluer les risques d'atteinte cognitive. Des evaluations d'impact pourraient examiner l'addiction, la polarisation, la desinformation, les effets sur les mineurs, la manipulation emotionnelle et les choix par defaut.

5.4 Transparence, controle et desactivation

Les utilisateurs devraient savoir quand un contenu est personnalise, pourquoi certaines recommandations apparaissent et comment desactiver ou reinitialiser la personnalisation. Les plateformes devraient offrir des options simples, visibles et comprehensibles.

5.5 Application et recours

Les organismes existants - commissaires a la vie privee, bureaux de concurrence, organismes de protection du consommateur et tribunaux des droits - pourraient recevoir des mandats explicites pour examiner les pratiques affectant l'autonomie cognitive. Les recours pourraient inclure injonctions, dommages statutaires, ordonnances de divulgation, audits obligatoires et sanctions administratives.

6. Feuille de route de mise en oeuvre

- Phase 1 - Sensibilisation: publier des notes de recherche, organiser des discussions avec juristes, chercheurs, organismes civiques et specialistes de l'IA.
- Phase 2 - Definitions: tester les termes "liberte cognitive", "integrite cognitive", "vie privee mentale" et "manipulation cognitive" dans des contextes canadiens.
- Phase 3 - Propositions legislatives: rediger des clauses pouvant etre integrees a des lois sur l'IA, la protection de la vie privee, la consommation ou les droits de la personne.
- Phase 4 - Protocoles de preuve: developper des methodes de conservation, d'audit et d'analyse pour documenter les environnements d'influence.
- Phase 5 - Application pilote: experimenter des lignes directrices, audits publics, etiquettes d'influence et voies de recours proportionnees.

Annexe A - Breve note de sensibilisation juridique

Question: Les technologies modernes peuvent influencer les pensees, emotions et decisions d'une personne d'une maniere que le droit canadien ne nomme pas encore clairement.

Concepts cles: La liberte cognitive designe l'autonomie de l'esprit; l'integrite cognitive designe la protection contre les interferences non justifiees; la vie privee mentale designe la protection des donnees, profils et inférences qui revelent les etats internes.

Pourquoi cela importe: Le consentement, la capacite, la responsabilite civile, la vie privee, la concurrence et les droits de la personne reposent sur l'idee que les individus peuvent comprendre et choisir. Si l'environnement de choix est concu pour contourner la comprehension, ces categories doivent etre reexaminees.

- Discuter des liens avec les pratiques existantes: vie privee, cybersecurite, IA, litige, consommation, droit public et droits de la personne.
- Developper des hypotheses prudentes: contrats obtenus par dark patterns, publicite psychographique, recommandations dommageables, profilage de vulnerabilites.
- Collaborer avec des experts: psychologues, scientifiques des donnees, specialistes UX, juristes, chercheurs en politiques publiques.

Annexe B - Feuille d'engagement pour cabinets juridiques

Cognitive Security Canada propose de developper un cadre de recherche sur la liberte cognitive au Canada. Les cabinets peuvent contribuer en validant les definitions, en testant les hypotheses juridiques, en suggerant des voies de recours et en participant a des tables rondes sur l'influence numerique et le droit.

- Consentement: quand une interface rend le refus couteux, le consentement reste-t-il reel?
- Capacite: comment evaluer une decision prise sous pression algorithmique, fatigue ou confusion intentionnelle?
- Responsabilite: quel devoir de diligence pour une plateforme qui connait les effets previsibles de son design?
- Preuve: quelles donnees doivent etre conservees pour demontrer une influence cumulative?

Annexe C - Clauses statutaires illustratives

Definition: "Liberte cognitive" signifie le droit de toute personne a l'autonomie de ses processus mentaux, y compris la liberte de penser, de croire, d'interpreter, de douter et de decider sans manipulation technologique non consentie.

Manipulation cognitive: utilisation d'un logiciel, d'un algorithme, d'une application, d'une interface ou d'un dispositif pour influencer de facon importante les pensees, perceptions, croyances ou decisions d'une personne sans consentement eclaire.

Droit a l'integrite cognitive: Nul ne peut, sans consentement, utiliser des moyens technologiques pour entraver de facon materielle la capacite d'une personne a penser de maniere autonome ou a prendre une decision libre et informee.

Obligation des fournisseurs: Les fournisseurs de services numeriques doivent prendre des mesures raisonnables pour proteger l'autonomie cognitive des utilisateurs, notamment par des evaluations d'impact, la transparence de la personnalisation, l'evitement des dark patterns et des options faciles de retrait.

Annexe D - Protocole de preuve: documenter l'interference cognitive

- Conserver les journaux de contenu: publicites, recommandations, notifications, messages, captures d'ecran et horodatages.
- Construire une chronologie: exposition, reactions, decisions, changements de comportement et consequences observees.
- Auditer les algorithmes lorsque possible: tests controles, comparaison de profils et analyses par experts independants.
- Evaluer les effets psychologiques avec prudence: distinguer correlation, contribution probable et causalite etablie.
- Comparer avec des groupes ou profils temoins: detecter si certaines vulnerabilites declenchent des contenus differents.
- Obtenir les politiques et documents internes pertinents: conditions d'utilisation, politiques de ciblage, guides de design et rapports de risque.

- Utiliser la divulgation juridique ou les pouvoirs reglementaires pour obtenir les elements necessaires tout en respectant la vie privee.

References selectionnees

- Ministere de la Justice Canada - Charterpedia, article 7: vie, liberte et securite de la personne.
- Emily Laidlaw, Technology-Facilitated Mind Hacking: Protection of Inner Freedoms in Canadian Law, CIGI Policy Brief, 2024.
- Susie Alegre et Aaron Shull, Freedom of Thought: Reviving and Protecting a Forgotten Human Right, CIGI Special Report, 2024.
- Gouvernement du Canada, Office de la consommation - Dark patterns.
- UK Online Safety Act, 2023.
- Australian Human Rights Commission, Protecting Cognition: Neurotechnology and Human Rights.
- Commissariat a la protection de la vie privee du Canada, Hacking the Human Mind: Lessons for Canada's Democracy.
- Documents federaux sur l'Artificial Intelligence and Data Act (AIDA).

Fin de la version francaise.