

CONNEXION-U — CAMPAGNE 2026

DÉVELOPPEMENT

Souveraineté numérique : protéger le choix avant que le choix disparaisse

La campagne 2026 de Connexion-U ne part pas d'une opposition à la technologie.

Elle part d'une question beaucoup plus simple :

À QUEL MOMENT UN CHOIX THÉORIQUEMENT LIBRE CESSE-T-IL DE L'ÊTRE PARCE QUE LES CONDITIONS MATÉRIELLES QUI PERMETTAIENT DE CHOISIR ONT DISPARU?

Depuis 2022, Connexion-U analyse, documente et éprouve sur le terrain les transformations qui touchent la protection des renseignements personnels, l'accès aux services financiers, l'argent comptant, l'identité numérique et, maintenant, l'interopérabilité.

Elle part de situations concrètes rencontrées par les citoyens : consentir pour accéder à son compte, fournir des renseignements personnels, trouver un guichet, obtenir un service humain, utiliser de l'argent comptant, s'identifier auprès d'une institution ou accéder à un service numérisé.

À mesure que la même logique de collecte s'est étendue aux institutions, aux services publics et au commerce, une question plus vaste est apparue :

Que devient le choix lorsque toutes les voies conduisent progressivement vers la même architecture numérique?

1. 2022 — PREMIER VERROU : L'AFFAIBLISSEMENT DU CONSENTEMENT

En 2022, Connexion-U s'est intéressé à une situation concrète vécue chez Desjardins.

La politique de confidentialité remise aux membres indiquait notamment que le consentement était « obligatoire pour faire affaire avec nous » et qu'un refus de transmettre certains renseignements pouvait empêcher Desjardins de fournir un produit ou un service.

La même politique affirmait pourtant ne recueillir que les renseignements personnels nécessaires.

UN CONSENTEMENT OBLIGATOIRE EST-IL ENCORE UN CONSENTEMENT?

La question juridique est plus précise encore.

La Loi sur la protection des renseignements personnels dans le secteur privé encadre la nécessité de la collecte et, pour les traitements qui reposent effectivement sur le consentement, exige aujourd'hui un consentement manifeste, libre, éclairé et donné à des fins spécifiques.

Le problème n'est donc pas de nier les obligations légales auxquelles une institution financière doit se conformer.

Une banque doit notamment vérifier certaines informations concernant ses clients.

Mais il faut pouvoir distinguer :

- ce que la loi exige;
- ce qui est nécessaire à l'exécution du service;
- ce que l'organisation choisit comme procédure;
- et ce qui demeure réellement facultatif.

Or le citoyen n'est généralement pas en mesure d'effectuer lui-même cette analyse.

Il reçoit une demande. On lui indique qu'elle est nécessaire ou obligatoire. L'employé ou le responsable applique la procédure qui lui a été transmise. L'organisation possède des spécialistes, des avocats, des systèmes informatiques et une autorité institutionnelle difficile à contester.

Le citoyen, lui, veut simplement accéder à son compte ou obtenir son service.

S'il conteste, il doit comprendre la loi, trouver la disposition applicable, distinguer une obligation réglementaire d'une politique interne et parfois déposer une plainte.

C'est précisément ce que Connexion-U a permis de faire collectivement en 2022. Après avoir analysé avec des experts les conditions dans lesquelles le consentement était demandé et les conséquences du refus sur l'accès aux comptes et à l'argent des citoyens, Connexion-U a mené une importante mobilisation afin d'accompagner les citoyens dans leurs démarches de plainte visant le Mouvement Desjardins et d'autres institutions bancaires canadiennes.

[Campagne Connexion-U 2022 — Le consentement](#)

LA PROTECTION NE PEUT PAS REPOSER SUR LA VIGILANCE JURIDIQUE DU CITOYEN.

Le citoyen n'a écrit ni la loi, ni le contrat, ni la procédure, ni le standard technique. Il n'a choisi ni le prestataire ni les sous-traitants. Il ne devrait donc pas lui appartenir de découvrir après coup qu'un renseignement n'était pas nécessaire ou qu'une procédure présentée comme obligatoire comportait en réalité plusieurs possibilités.

2. VÉRIFIER UNE IDENTITÉ NE SIGNIFIE PAS TOUT CONSERVER

Nos recherches sur les obligations fédérales des institutions financières ont permis de préciser considérablement cette question.

Le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) prévoit plusieurs méthodes de vérification de l'identité. Dans le cas d'une pièce d'identité gouvernementale avec photo, son authenticité peut notamment être vérifiée en personne, à partir du document physique. CANAFE impose alors la conservation de certains renseignements relatifs à la vérification — notamment le type de document et son numéro — mais cela n'équivaut pas, en soi, à une obligation de conserver une image intégrale de la pièce.

VOIR ≠ VÉRIFIER ≠ COPIER ≠ ENREGISTRER ≠ CONSERVER ≠ RELIER ≠ COMMUNIQUER

Chaque opération supplémentaire doit posséder sa propre justification.

La Commission d'accès à l'information du Québec (CAI) rappelle d'ailleurs que le simple fait de voir une pièce d'identité constitue déjà une collecte et que la nécessité doit être déterminée avant la collecte. Limiter la collecte réduit également les conséquences potentielles d'une fuite, d'une communication non autorisée ou d'une utilisation interdite.

La cybersécurité et la protection des renseignements personnels se rencontrent donc à certains endroits. Mais elles ne sont pas synonymes.

La cybersécurité peut nécessiter de vérifier qu'une personne est bien celle qu'elle prétend être. Cela ne signifie pas automatiquement : plus nous possédons de renseignements sur elle, plus elle est protégée.

Au contraire, chaque renseignement supplémentaire détenu élargit l'étendue des données exposées lorsqu'un système est compromis.

SÉCURISER UNE ARCHITECTURE NE SUFFIT PAS À JUSTIFIER TOUT CE QU'ELLE CONTIENT.

Elle doit commencer AVANT.

Avant la collecte inutile.

Avant la conservation inutile.

Avant la liaison inutile.

Avant que l'alternative disparaisse.

Avant que l'architecture devienne irréversible.

C'EST LE PRINCIPE DE PRÉVENTION.

3. L'ALTERNATIVE PERMANENTE

Cette analyse fait apparaître une distinction qui dépasse largement Desjardins.

Une loi peut obliger une organisation à vérifier une identité. Mais cela ne signifie pas automatiquement que le citoyen doit accepter toute méthode technologique choisie par cette organisation.

Lorsqu'une obligation légale exige de vérifier une identité ou un renseignement, elle ne doit pas être interprétée comme autorisant une collecte, une copie, une conservation ou une intégration numérique supplémentaire qui n'est pas elle-même nécessaire à cette obligation.

UNE VOIE PERMANENTE DE VÉRIFICATION HUMAINE OU ANALOGIQUE DOIT DEMEURER ACCESSIBLE.

Cela ne signifie pas supprimer les obligations d'identification. Cela signifie empêcher qu'une obligation de s'identifier devienne silencieusement une obligation d'être intégré numériquement.

4. 2024 — DEUXIÈME VERROU : L'ALTERNATIVE DISPARAÎT

En 2024, Connexion-U a rencontré le même problème sous une autre forme. Cette fois, il ne s'agissait plus seulement des renseignements personnels. Il s'agissait de l'argent et des services physiques.

Lorsque l'argent comptant existe encore juridiquement mais que les guichets, les comptoirs, les services humains et les possibilités de l'utiliser diminuent progressivement, le choix existe-t-il encore réellement?

Les institutions peuvent expliquer les fermetures par la diminution de l'achalandage. Mais il faut également pouvoir examiner le mécanisme inverse : que se passe-t-il lorsque les heures diminuent, que les employés deviennent moins nombreux, que les points de service fusionnent et que l'usage physique devient progressivement moins pratique?

La diminution de l'usage peut alors servir à justifier la diminution de l'offre, laquelle provoque à son tour une nouvelle diminution de l'usage.

Le choix existe encore sur papier. Mais sa condition matérielle disparaît.

UNE ALTERNATIVE QUI PEUT ÊTRE RENDUE INUTILISABLE N'EST PAS UNE VÉRITABLE ALTERNATIVE.

ET SANS ALTERNATIVE, NOUS NE POUVONS PLUS PARLER DE CHOIX.

L'ALTERNATIVE EST LA CONDITION MATÉRIELLE DU CHOIX.

Ce principe devient particulièrement important pour l'identité numérique.

Depuis le 28 octobre 2025, la loi québécoise prévoit expressément que l'utilisation de l'identité numérique nationale ne peut être imposée par un organisme public pour fournir une prestation gouvernementale.

C'est une protection importante. Mais elle ne répond pas entièrement à une autre question : l'alternative permettant de ne pas l'utiliser demeurera-t-elle matériellement accessible dans dix ans?

UNE IDENTITÉ NUMÉRIQUE N'EST RÉELLEMENT FACULTATIVE QUE SI LA VOIE PERMETTANT DE NE PAS L'UTILISER DEMEURE RÉELLEMENT DISPONIBLE.

5. 2026 — TROISIÈME VERROU : L'INTEROPÉRABILITÉ

En 2026, la recherche conduit Connexion-U à regarder une nouvelle étape.

Les systèmes bancaires, gouvernementaux, identitaires, transactionnels et privés deviennent de plus en plus capables de communiquer.

**DES BRIQUES CONSTRUITES SÉPARÉMENT PEUVENT MAINTENANT ÊTRE
INTERRELIÉES.**

La loi québécoise fournit elle-même un exemple concret de cette évolution.

Elle institue désormais un registre de l'identité numérique nationale pouvant permettre la conservation, la communication entre organismes publics, l'accès et la traçabilité des accès à certaines données numériques

gouvernementales. Elle confie également au ministre de la Cybersécurité et du Numérique la gouvernance et la gestion centralisée de l'identité numérique nationale.

Cela ne démontre pas l'existence d'un système unique contrôlant toutes les données des citoyens. Et ce n'est pas nécessaire pour que la question démocratique se pose.

DES SYSTÈMES QUI ÉTAIENT SÉPARÉS PEUVENT DEVENIR INTEROPÉRABLES.

Nos recherches sur les réseaux internationaux qui ont participé au développement de la monnaie numérique, de la traçabilité, de l'identité, des données et des infrastructures financières nous ont conduits à regarder les différentes briques non plus séparément, mais comme les composantes potentiellement interopérables d'une même architecture.

La question n'est donc plus seulement : « Cette brique est-elle légale? »

QUE PRODUIT L'ASSEMBLAGE DES BRIQUES?

Pourquoi relier ces renseignements, ces identités et ces systèmes? Dans quel but?

Quelles protections traversent toutes les composantes de cette architecture, peu importe qui construit chacune des briques?

6. LE PROBLÈME DU DROIT SECTORIEL

Nos lois contiennent déjà plusieurs protections. C'est une découverte importante de cette recherche. Il ne serait donc pas exact d'affirmer que le citoyen ne possède aucun droit.

Il existe notamment des règles concernant la nécessité, la minimisation, le consentement, la finalité, la conservation, la destruction, l'accès, la rectification et certaines communications à des tiers.

La CAI précise même que les obligations relatives à la collecte continuent de s'appliquer lorsque celle-ci est confiée à un tiers.

Mais ces protections ont été conçues dans différentes lois et différents secteurs, et leur application relève de différents organismes et autorités.

Pendant ce temps, les systèmes deviennent capables de communiquer au-delà de leurs frontières juridiques et institutionnelles.

QUI PROTÈGE LE CITOYEN LORSQUE TOUTES CES RELATIONS COMMENCENT À SE CROISER?

Connexion-U n'a trouvé aucun droit transversal garantissant l'ensemble des protections nécessaires à travers l'architecture interopérable.

Le droit transversal ne vise donc pas à réinventer les protections existantes. Il vise à garantir :

- que les protections existantes continuent de produire leurs effets lorsque plusieurs systèmes deviennent interopérables;
- que d'autres protections les renforcent;
- que des protections soient créées lorsque l'assemblage des briques produit des capacités qui n'existaient pas lorsque les règles sectorielles ont été conçues.

7. LA LISTE DE VÉRIFICATION DES CONSÉQUENCES NUMÉRIQUES

Le premier outil proposé par Connexion-U pour rendre ce droit concret est une Liste de vérification des conséquences numériques.

Elle ne crée pas le droit à l'information. Elle rend visible, compréhensible et vérifiable avant l'acceptation ce que nos lois reconnaissent déjà, puis le complète lorsque l'interopérabilité produit des conséquences que les règles sectorielles ne rendent pas visibles.

Il ne s'agit pas d'un autre contrat de neuf pages. Ni d'une politique de confidentialité de trente pages. Ni d'une fenêtre disant simplement : « Nos conditions ont changé. »

La Liste de vérification doit permettre au citoyen — mais aussi à l'employé qui applique la procédure — de voir immédiatement :

- QUI DÉCIDE?
- QUI L'EXIGE?
- EN VERTU DE QUELLE LOI?
- POUR QUELLE FINALITÉ?
- CE RENSEIGNEMENT EST-IL NÉCESSAIRE AU SERVICE?
- EST-CE UNE OBLIGATION LÉGALE OU UN CHOIX DE L'ORGANISATION?
- FAUT-IL LE VÉRIFIER, LE COPIER OU LE CONSERVER?
- L'INTÉGRATION NUMÉRIQUE EST-ELLE NÉCESSAIRE?
- À QUEL TIERS SERA-T-IL COMMUNIQUÉ?
- POURQUOI CE TIERS EST-IL NÉCESSAIRE?
- QUELS RENSEIGNEMENTS PRÉCIS POURRA-T-IL RECEVOIR?
- COMBIEN DE TEMPS SERONT-ILS CONSERVÉS?
- QUE SE PASSE-T-IL ENSUITE?
- QUE SE PASSE-T-IL SI JE REFUSE?
- AI-JE TOUJOURS ACCÈS AU SERVICE?
- QUELLE ALTERNATIVE M'EST OFFERTE?
- COMMENT SORTIR?
- COMMENT SAVOIR QUE LA DESTRUCTION A EFFECTIVEMENT ÉTÉ EXÉCUTÉE?

La Liste de vérification doit également distinguer chaque finalité réelle. Par exemple :

- Nécessaire au service — OUI/NON — justification : _____
- Exigé par une loi — OUI/NON — loi : _____
- Copie de la pièce requise — OUI/NON — justification : _____
- Conservation de l'identifiant — OUI/NON — durée : _____
- Publicité personnalisée — ☐ J'accepte ☐ Je refuse
- Analyse de comportement — ☐ J'accepte ☐ Je refuse
- Communication à un tiers — ☐ J'accepte ☐ Je refuse, lorsque le consentement constitue réellement la base applicable

La Liste de vérification doit être fournie avant l'acceptation. Pas lorsque le citoyen découvre le problème. Pas après la plainte. Pas après avoir consulté un avocat.

RENDRE REFUSABLE CE QUI RELÈVE RÉELLEMENT DU CHOIX EN LE SÉPARANT DE CE QUI EST VÉRITABLEMENT IMPOSÉ PAR LA LOI.

8. QUI DÉCIDE DES TIERS?

L'interopérabilité rend également insuffisante une formule générale comme : « Nous pouvons communiquer vos renseignements à des fournisseurs ou partenaires. »

- Qui a décidé que ce tiers devait intervenir?
- Pourquoi son intervention est-elle nécessaire?
- Quels renseignements précis doit-il recevoir?
- Peut-il les transmettre à un sous-traitant?
- Où seront-ils traités?
- Combien de temps seront-ils conservés?
- Comment l'organisation vérifie-t-elle leur destruction?

COMMENT LA PERSONNE CONCERNÉE PEUT-ELLE SAVOIR QUE CETTE DESTRUCTION A EU LIEU?

Une obligation juridique de détruire n'est pas la même chose qu'une preuve accessible de son exécution.

LA TRAÇABILITÉ DE LA DESTRUCTION

Le citoyen ne devrait pas avoir à auditer lui-même tous les prestataires. La responsabilité doit demeurer du côté de l'organisation qui a décidé de recueillir, conserver et communiquer le renseignement.

9. DÉSABONNEMENT ≠ DESTRUCTION

Cette distinction mérite également d'être expliquée au public.

Lorsqu'une personne clique sur « se désabonner » d'une liste de courriels, elle peut croire qu'elle a retiré ses renseignements de l'organisation. Ce n'est pas nécessairement le cas.

Le désabonnement peut simplement signifier : « ne plus utiliser mon adresse pour m'envoyer cette catégorie de communications ». Il ne signifie pas automatiquement : « supprimer tous les renseignements que vous détenez à mon sujet ».

Cette distinction montre pourquoi la culture numérique doit évoluer.

Le citoyen doit pouvoir comprendre non seulement ce qu'il accepte, mais ce qui arrive réellement à ses renseignements lorsqu'il refuse, se désabonne, retire un consentement ou quitte un service.

À LA CULTURE DE L'ÉCONOMIE NUMÉRISÉE DOIT RÉPONDRE UNE CULTURE DU CHOIX ET DES CONTRE-POUVOIRS.

10. LA CHARTE QUÉBÉCOISE DE GARANTIES NUMÉRIQUES

Pour éviter qu'un troisième verrou ne devienne permanent, Connexion-U propose que le Québec se dote d'une Charte québécoise de garanties numériques fondée sur un droit transversal.

1. Le libre choix technologique.

Aucune personne ne devrait être privée d'un service public ou essentiel du seul fait qu'elle refuse un moyen d'identification numérique. Une voie permanente, humaine ou analogique, doit être maintenue afin de permettre l'établissement des renseignements légalement nécessaires à la prestation du service.

2. Une alternative permanente, humaine ou analogique.

Cette alternative doit demeurer matériellement accessible et permettre de fournir les renseignements légalement nécessaires sans imposer une intégration numérique supplémentaire non nécessaire.

3. L'interdiction de provoquer silencieusement l'attrition de l'alternative.

Une alternative ne doit pas pouvoir disparaître progressivement par fermeture des comptoirs, réduction de l'accès, choix technologique, objectif de numérisation, recherche d'efficacité administrative, invocation de la sécurité ou de la cybersécurité, ni par tout autre objectif institutionnel qui aurait pour effet de rendre cette alternative impraticable.

4. L'indépendance entre cybersécurité et nécessité des renseignements.

Une justification de sécurité ne doit pas automatiquement autoriser une collecte plus vaste. La nécessité et la minimisation doivent demeurer des tests autonomes.

5. La Liste de vérification des conséquences numériques.

Les obligations légales, choix institutionnels, finalités, tiers, conséquences, possibilités de refus et portes de sortie doivent être compréhensibles avant l'acceptation.

6. La séparation fonctionnelle.

L'identité, le paiement, le profilage, l'authentification et l'accès aux services ne doivent pas être reliés simplement parce que la technologie permet de le faire.

7. Une gouvernance démocratique de l'interopérabilité.

L'assemblage de systèmes produisant une nouvelle capacité importante doit être identifiable, auditable et soumis à une responsabilité politique claire.

8. Une garantie transversale de réversibilité.

Les droits existants concernant le consentement, la nécessité, la conservation et la destruction doivent continuer à pouvoir être exercés lorsque les renseignements sont intégrés à plusieurs systèmes, sans perte injustifiée de l'accès au service ou au bien.

9. Une traçabilité vérifiable de la destruction.

Lorsqu'un renseignement doit être détruit, l'organisation doit pouvoir démontrer que cette obligation a été exécutée dans la chaîne pertinente.

10. Un recours humain accessible de manière permanente.

Il doit être possible non seulement de déposer une plainte, mais de rétablir rapidement l'accès lorsqu'un citoyen est bloqué par une procédure, une technologie ou une décision automatisée.

11. Des contre-pouvoirs capables d'auditer l'architecture une fois les briques assemblées.

Ils doivent pouvoir déterminer si l'assemblage de composantes individuellement légales produit une capacité nouvelle qui n'a jamais été explicitement débattue ou autorisée.

12. Une protection contre la disparition silencieuse des garanties.

Toute mesure ayant pour effet de réduire substantiellement une garantie numérique fondamentale devrait identifier explicitement la garantie touchée, la justification de cette réduction et sa portée.

11. QUI PROTÈGE LES PROTECTIONS?

Aucune loi ordinaire ne peut empêcher définitivement une future Assemblée nationale de la modifier.

La question n'est donc pas de prétendre rendre ces garanties éternelles.

COMMENT RENDRE LEUR SUPPRESSION POLITIQUEMENT VISIBLE, JURIDIQUEMENT EXPLICITE ET INSTITUTIONNELLEMENT DIFFICILE À ACCOMPLIR SILENCIEUSEMENT?

Une protection fondamentale ne devrait pas pouvoir disparaître simplement parce qu'un règlement change, qu'un fournisseur modifie son architecture, qu'une administration ferme progressivement ses comptoirs ou qu'une justification générale de cybersécurité est invoquée.

Si une autorité veut réduire une garantie, elle devrait devoir l'assumer : dire quelle garantie est touchée; pourquoi; pour quelle finalité; pour quelle durée; et pourquoi une solution moins attentatoire ne permet pas d'atteindre le même objectif.

Il faut également éviter de confier exclusivement la protection de ces droits aux autorités dont la mission consiste simultanément à développer, promouvoir ou sécuriser l'infrastructure numérique.

LE CONTRE-POUVOIR DOIT POUVOIR REGARDER L'ARCHITECTURE DE L'EXTÉRIEUR.

12. LA QUESTION DE 2026

La modernisation peut avancer. L'innovation peut avancer. La cybersécurité doit avancer.

MAIS ELLES NE DOIVENT PAS POUVOIR DÉTRUIRE LA VOIE PERMETTANT DE LES REFUSER LORSQU'ELLE N'EST PAS JURIDIQUEMENT NÉCESSAIRE.

En 2022, Connexion-U a rencontré l'affaiblissement du consentement.

En 2024, la disparition progressive des alternatives physiques.

En 2026, l'interopérabilité révèle que ces problèmes peuvent devenir les différentes étapes d'un même mécanisme :

**COLLECTER → IDENTIFIER → CONSERVER → RELIER → RENDRE L'ALTERNATIVE
IMPRATICABLE → RENDRE LA SORTIE IMPOSSIBLE**

C'est ce troisième verrou qu'il faut empêcher avant qu'il ne devienne matériellement irréversible.

Et derrière toute la campagne de Connexion-U demeure une question :

POUVONS-NOUS TOUJOURS CONSERVER NOTRE SOUVERAINETÉ NUMÉRIQUE?