

**CONNEXION-U**

**CAMPAGNE 2026**

# Souveraineté numérique

**Protéger le choix avant  
que le choix disparaisse**



## **DOSSIER COMPLET**

Lettre · Sommaire · Développement  
Annexe juridique et documentaire

[connexion-u.org/souverainete-numerique/](https://connexion-u.org/souverainete-numerique/)

## **Objet : Souveraineté numérique — protéger le choix avant que le choix disparaisse**

Madame, Monsieur,

Depuis 2022, Connexion-U analyse, documente et éprouve sur le terrain les transformations qui touchent la protection des renseignements personnels, l'accès à l'argent, les services essentiels et la numérisation de l'économie québécoise.

Ce travail prolonge une réflexion amorcée dès 2019 avec notre Déclaration sur l'être essentiel et ses huit principes. Devant l'accélération technologique, elle posait déjà une question fondamentale : quelles conditions doivent demeurer sous le pouvoir de l'être humain afin qu'il conserve réellement sa capacité de choisir?

La confrontation de ces principes aux réalités du terrain nous a progressivement permis d'identifier trois moments charnières :

### **2022 — Le consentement disparaît 2024 — L'argent disparaît 2026 — L'interopérabilité nous verrouille, le choix disparaît**

Ces trois étapes nous amènent aujourd'hui à interpeller les candidates et candidats aux prochaines élections québécoises.

Nos lois accordent déjà aux citoyens d'importantes protections en matière de renseignements personnels. Elles encadrent notamment la nécessité de la collecte, le consentement, la conservation, la destruction et certaines communications de renseignements.

Mais, parallèlement, les systèmes bancaires, gouvernementaux, identitaires, transactionnels et privés deviennent de plus en plus capables de communiquer.

#### **Des briques construites séparément peuvent maintenant être interreliées.**

Une nouvelle question politique apparaît alors :

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

Notre analyse nous conduit à constater qu'il manque aujourd'hui un droit transversal capable de garantir que les protections existantes continueront de produire leurs effets lorsque les systèmes deviennent interopérables — et que le citoyen conservera réellement une alternative et une porte de sortie.

Cette question devient d'autant plus importante lorsque la voie permettant de refuser le numérique disparaît progressivement.

Une identité numérique peut être facultative en droit. L'argent comptant peut continuer d'exister. Un service humain peut théoriquement demeurer disponible.

Mais si les comptoirs ferment, si les guichets disparaissent, si les procédures analogiques deviennent impraticables ou si le refus d'une intégration numérique empêche d'accéder au service, le choix existe-t-il encore réellement?

Pour Connexion-U, un principe doit désormais guider la transformation numérique du Québec :

#### **L'ALTERNATIVE EST LA CONDITION MATÉRIELLE DU CHOIX.**

C'est pourquoi Connexion-U soumet aux candidates et candidats une proposition de Charte québécoise de garanties numériques, reposant notamment sur une alternative permanente, humaine ou analogique; une Liste de vérification des conséquences numériques; la réversibilité; un encadrement démocratique de l'interopérabilité; un recours humain effectif; et des contre-pouvoirs capables d'auditer l'architecture une fois les briques assemblées.

Cette proposition n'est pas une opposition à la modernisation ni à la cybersécurité.

#### **LA MODERNISATION PEUT AVANCER.**

#### **MAIS ELLE NE DOIT PAS POUVOIR DÉTRUIRE LA VOIE PERMETTANT DE LA REFUSER LORSQU'ELLE N'EST PAS JURIDIQUEMENT NÉCESSAIRE.**

Nous vous invitons à prendre connaissance du Sommaire de la campagne 2026, de son développement et de son dossier juridique et documentaire :

<https://connexion-u.org/souverainete-numerique/>

Nous vous transmettrons également un questionnaire afin de connaître clairement vos engagements sur ces enjeux avant le scrutin.

Les électrices et électeurs doivent pouvoir savoir quelles candidates et quels candidats sont prêts à garantir que la transformation numérique du Québec ne fera pas disparaître silencieusement le choix que nos lois protègent encore.

La question qui traverse l'ensemble de notre démarche est finalement très simple :

**POUVONS-NOUS TOUJOURS CONSERVER NOTRE SOUVERAINETÉ NUMÉRIQUE?**

Connexion-U <https://connexion-u.org/souverainete-numerique/>

# CONNEXION-U — CAMPAGNE 2026 SOMMAIRE AUX CANDIDATES ET CANDIDATS

## Souveraineté numérique : protéger le choix avant que le choix disparaisse

Depuis 2022, Connexion-U analyse, documente et éprouve sur le terrain les transformations qui touchent la protection des renseignements personnels, l'accès à l'argent, les services essentiels et la numérisation de l'économie.

Ce travail nous a permis d'identifier trois moments charnières :

|                                                 |                                          |                                                                                  |
|-------------------------------------------------|------------------------------------------|----------------------------------------------------------------------------------|
| <b>2022</b><br><b>Le consentement disparaît</b> | <b>2024</b><br><b>L'argent disparaît</b> | <b>2026</b><br><b>L'interopérabilité nous verrouille,<br/>le choix disparaît</b> |
|-------------------------------------------------|------------------------------------------|----------------------------------------------------------------------------------|

Ces trois moments révèlent un même problème sous des formes différentes :

### **UN DROIT PEUT CONTINUER D'EXISTER JURIDIQUEMENT TOUT EN DEVENANT PROGRESSIVEMENT PLUS DIFFICILE À EXERCER MATÉRIELLEMENT.**

En 2022, la question portait sur les conditions d'un consentement réellement libre et éclairé.

En 2024, elle portait sur la disparition progressive des alternatives physiques au numérique.

En 2026, elle porte sur ce qui arrive lorsque des systèmes jusque-là séparés deviennent capables de communiquer entre eux.

### **L'ALTERNATIVE EST LA CONDITION MATÉRIELLE DU CHOIX.**

## 2026 — QUE CHANGE L'INTEROPÉRABILITÉ?

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 question n'est donc plus seulement de savoir si chaque système respecte séparément les règles qui lui sont applicables.

Elle devient :

### **QUE DEVIENNENT LES PROTECTIONS EXISTANTES LORSQUE LES BRIQUES DE L'ARCHITECTURE NUMÉRIQUE, CONÇUES SÉPARÉMENT, S'ASSEMBLENT ET DEVIENNENT CAPABLES DE COMMUNIQUER ENTRE ELLES?**

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?

Nos lois contiennent déjà plusieurs protections importantes. Mais elles sont réparties entre différentes lois, différents secteurs et différentes autorités.

**Connexion-U n'a trouvé aucun droit transversal garantissant que l'ensemble des protections nécessaires continuera de produire ses effets lorsque les systèmes deviennent interopérables.**

## CONNEXION-U PROPOSE UN DROIT TRANSVERSAL

Ce droit ne remplacerait pas les protections qui existent déjà. Il viserait à faire en sorte qu'elles traversent les briques, demeurent visibles et puissent réellement être exercées lorsque plusieurs systèmes deviennent interopérables.

|                                                                                                                                             |                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>CHOIX</b><br>Pouvoir accepter ou refuser ce qui n'est pas juridiquement nécessaire.                                                      | <b>MINIMISATION</b><br>Ne recueillir et ne conserver que les renseignements nécessaires.                 |
| <b>SÉPARATION DES FONCTIONS</b><br>Ne pas relier automatiquement des renseignements simplement parce que la technologie permet de le faire. | <b>ALTERNATIVE PERMANENTE</b><br>Maintenir une voie humaine ou analogique réellement accessible.         |
| <b>RÉVERSIBILITÉ</b><br>Pouvoir retirer ou dissocier ce qui n'a plus à être lié ou conservé selon le droit applicable.                      | <b>PORTE DE SORTIE</b><br>Pouvoir sortir d'une architecture sans perdre indûment l'accès au service.     |
| <b>RECOURS HUMAIN</b><br>Pouvoir joindre une personne capable de rétablir concrètement un droit ou un accès.                                | <b>CONTRE-POUVOIRS</b><br>Pouvoir auditer ce que produit l'architecture une fois les briques assemblées. |

## COMMENT RENDRE CE DROIT CONCRET?

### 1. UNE LISTE DE VÉRIFICATION DES CONSÉQUENCES NUMÉRIQUES

Elle permettrait de distinguer clairement, avant l'acceptation : qui exige le renseignement; en vertu de quoi; pour quelle finalité; ce qui est réellement obligatoire; ce qui relève d'un choix de l'organisation; ce qui sera vérifié, copié, conservé ou communiqué; quels tiers interviennent; combien de temps le renseignement sera conservé; ce qui arrive en cas de refus; quelle alternative humaine ou analogique demeure disponible; et comment sortir lorsque le lien n'est plus justifié.

### 2. UNE ALTERNATIVE PERMANENTE

Une personne ne devrait pas pouvoir être privée d'un service public ou essentiel du seul fait qu'elle refuse un moyen d'identification numérique. Une voie humaine ou analogique doit demeurer accessible pour fournir les renseignements légalement nécessaires.

**Une alternative qui peut être rendue inutilisable n'est pas une véritable alternative.**

### 3. UN ENCADREMENT DÉMOCRATIQUE DE L'INTEROPÉRABILITÉ

Même lorsque deux renseignements peuvent légalement être détenus séparément, leur liaison peut créer une capacité nouvelle. Il faut donc pouvoir répondre clairement : qui a autorisé la liaison; pourquoi elle est nécessaire; pour quelle finalité; quels renseignements deviennent accessibles; à qui; et avec quelles limites.

### 4. UNE RÉVERSIBILITÉ RÉELLE

Les protections concernant le consentement, la nécessité, la conservation et la destruction doivent continuer de pouvoir être exercées lorsque les renseignements sont intégrés à plusieurs systèmes. La personne doit pouvoir

savoir ce qui peut être retiré, dissocié ou détruit — et pourquoi une opération serait juridiquement impossible lorsqu'elle ne peut l'être.

## 5. UNE DESTRUCTION VÉRIFIABLE

Une obligation de destruction n'est pas la même chose qu'une preuve accessible que cette destruction a effectivement eu lieu. Le citoyen doit pouvoir connaître ce qui est encore détenu; par qui; jusqu'à quand; et ce qui se produit à l'échéance.

## 6. DES CONTRE-POUVOIRS INDÉPENDANTS

Il ne suffit plus d'auditer chaque brique séparément. Il faut aussi pouvoir examiner ce que produit leur assemblage. Un contre-pouvoir indépendant doit pouvoir déterminer si des composantes individuellement autorisées créent, une fois reliées, une capacité nouvelle qui n'a jamais été explicitement débattue ou autorisée.

### CE QUE PRODUIT LEUR ASSEMBLAGE.

**LE PRINCIPE QUI TRAVERSE TOUTE LA CAMPAGNE PEU IMPORTE QUI CONSTRUIT LA BRIQUE, ELLE NE PEUT SUPPRIMER LE CHOIX, L'ALTERNATIVE ET LA PORTE DE SORTIE.**

**Ce sont des conditions essentielles pour atteindre réellement la souveraineté numérique.**

**LA QUESTION POSÉE AUX CANDIDATES ET CANDIDATS ÊTES-VOUS PRÊTS À GARANTIR QUE LA TRANSFORMATION NUMÉRIQUE DU QUÉBEC NE POURRA PAS FAIRE DISPARAÎTRE SILENCIEUSEMENT LE CHOIX QUE NOS LOIS PROTÈGENT DÉJÀ?**

**Et, ultimement :**

**POUVONS-NOUS TOUJOURS CONSERVER NOTRE SOUVERAINETÉ NUMÉRIQUE?**

## 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 DISPARÂÎT**

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 RELEVÉ 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?**

## CONNEXION-U — CAMPAGNE 2026

## ANNEXE JURIDIQUE ET DOCUMENTAIRE

Souveraineté numérique — Fondements, distinctions et garanties transversales

Cette annexe distingue les protections déjà présentes dans le droit applicable, les constats documentaires issus du corpus de Connexion-U et les garanties nouvelles proposées par la campagne.

Son objectif n'est pas de prétendre que les protections juridiques n'existent pas. Au contraire, notre recherche montre qu'un nombre important d'entre elles existent déjà.

Le problème apparaît lorsqu'elles sont réparties entre différentes lois, différents organismes, différents secteurs et différentes autorités, alors que les systèmes, eux, deviennent progressivement capables de communiquer entre eux.

### QUE DEVIENNENT LES PROTECTIONS EXISTANTES LORSQUE LES BRIQUES S'ASSEMBLENT?

#### A. LA NÉCESSITÉ PRÉCÈDE LE CONSENTEMENT

La Loi sur la protection des renseignements personnels dans le secteur privé impose un principe fondamental : une organisation doit déterminer les fins de la collecte et ne recueillir que les renseignements nécessaires à ces fins. La nécessité ne naît donc pas du simple fait qu'un formulaire, un contrat ou un système informatique permet de demander un renseignement.

La Commission d'accès à l'information du Québec (CAI) rappelle également que le questionnaire sur la nécessité précède le consentement lorsqu'un consentement est applicable.

**La Liste de vérification des conséquences numériques ne créerait pas le principe de nécessité. Elle rendrait visible, compréhensible et vérifiable avant l'acceptation ce que nos lois reconnaissent déjà, puis le compléterait lorsque l'interopérabilité produit des conséquences que les règles sectorielles ne rendent pas visibles.**

**EXIGÉ PAR LA LOI ≠ NÉCESSAIRE AU SERVICE ≠ CHOISI PAR L'ORGANISATION ≠ IMPOSÉ PAR LE SYSTÈME INFORMATIQUE**

Source — [Loi sur la protection des renseignements personnels dans le secteur privé](#)

#### B. VÉRIFICATION BANCAIRE : CE QUE CANAFE EXIGE RÉELLEMENT

Le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) prévoit plusieurs méthodes permettant de vérifier l'identité d'une personne.

Lorsqu'une pièce d'identité gouvernementale avec photo est utilisée, son authenticité peut notamment être vérifiée en personne, en examinant le document physique original et ses caractéristiques de sécurité. CANAFE exige alors que

certains renseignements relatifs à la vérification soient consignés, notamment le type et le numéro du document ainsi que certaines informations sur sa délivrance.

**VÉRIFIER ≠ COPIER ≠ NUMÉRISER LA PIÈCE ENTIÈRE ≠ CONSERVER UNE IMAGE DE LA PIÈCE**

La vérification physique possible ne signifie donc pas absence de toute conservation réglementaire. Inversement, l'obligation de consigner certains renseignements ne démontre pas une obligation générale de conserver une copie numérique intégrale de la pièce.

CANAFE permet également plusieurs méthodes de vérification : document gouvernemental avec photo, dossier de crédit, processus double et autres méthodes prévues par son cadre. Cette pluralité ne donne toutefois pas automatiquement au client un droit général d'imposer à l'institution la méthode qu'il préfère.

C'est précisément l'un des espaces que l'Alternative permanente proposée par Connexion-U cherche à encadrer.

Source — CANAFE : méthodes de vérification de l'identité

## C. LE CAS DESJARDINS 2022 : L'ÉPREUVE DU CONSENTEMENT

Le document de confidentialité remis aux membres de Desjardins en 2022 présentait notamment le consentement comme « obligatoire pour faire affaire avec nous » et décrivait les conséquences possibles du refus de fournir certains renseignements.

Le document regroupait également de nombreuses catégories de renseignements et de finalités.

Une prudence demeure nécessaire : la présence d'une catégorie de renseignements dans une politique générale ne démontre pas, à elle seule, que chacun de ces renseignements était exigé de chaque membre pour chaque produit.

### Quel renseignement est réellement exigé? Par qui? En vertu de quelle disposition?

**Pour quelle finalité? Et quelle partie de la collecte résulte plutôt d'un choix contractuel, organisationnel ou technologique?**

Le problème rencontré en 2022 devient ainsi un cas d'épreuve du droit transversal. L'obligation légitime d'identifier un client ne devrait pas automatiquement devenir une autorisation d'intégrer numériquement davantage de renseignements que ce qui est juridiquement nécessaire.

**Campagne Connexion-U 2022 — Le consentement**

## D. DU COMMERCE AU PROFESSIONNEL : QUAND LA PROCÉDURE DEVIENT UNE OBLIGATION APPARENTE

La collecte numérique ne se limite plus aux banques et aux gouvernements.

Dans un commerce physique, une situation est devenue banale : pour mettre un article de côté, effectuer une réservation ou accomplir une opération simple, l'employé peut se trouver devant un système exigeant obligatoirement un nom, un numéro de téléphone ou une adresse courriel.

### UN CHAMP OBLIGATOIRE DANS UN LOGICIEL N'EST PAS, À LUI SEUL, UNE OBLIGATION LÉGALE.

La nécessité doit être établie en fonction de la finalité poursuivie. Pourquoi le courriel est-il demandé? Pourquoi le numéro de téléphone est-il demandé? Est-il nécessaire pour fournir le bien ou le service? Une loi l'exige-t-elle? Ou le logiciel a-t-il simplement été configuré pour empêcher l'employé de poursuivre sans remplir le champ?

Cette distinction protège également l'employé. Il peut croire de bonne foi qu'un renseignement est obligatoire simplement parce que son outil de travail l'exige. La culture de la collecte peut ainsi se propager sans que ni l'employé ni le client ne sachent exactement où se situe l'obligation juridique.

### Commerce en ligne

Dans le commerce électronique, certains renseignements peuvent évidemment être nécessaires à l'exécution de la transaction : paiement, livraison, facturation ou autres nécessités selon le contexte. Mais cela ne rend pas automatiquement nécessaires toutes les autres opérations qui peuvent accompagner la transaction.

### UNE POLITIQUE DE COMMERCE PRIVÉ N'EST PAS SYNONYME DE POLITIQUE GOUVERNEMENTALE, NI D'OBLIGATION LÉGALE.

Il faut distinguer notamment : acheter; créer un compte; conserver les coordonnées; conserver un moyen de paiement; analyser le comportement; profiler; communiquer à des tiers; utiliser à des fins commerciales.

La Liste de vérification doit précisément empêcher qu'une conséquence soit dissimulée derrière une catégorie générale.

## E. L'AUTORITÉ APPARENTE : ORDRES ET PROFESSIONS RÉGLEMENTÉES

Le même phénomène devient plus difficile à contester lorsqu'il se produit dans une profession réglementée.

Un notaire, un courtier hypothécaire ou un autre professionnel peut effectivement être soumis à des obligations légales et réglementaires de vérification, de collecte et de conservation.

La Chambre des notaires du Québec indique par exemple que le notaire doit vérifier l'identité au moyen de pièces admissibles et conserver une preuve de cette vérification. Elle précise qu'une preuve peut notamment prendre la forme d'une photocopie des pièces ou des informations qu'elles contiennent; elle reconnaît également la vérification en présence du client.

### Source — Chambre des notaires : obligation d'identification officielle

En courtage hypothécaire, l'Autorité des marchés financiers encadre aussi la collecte de renseignements nécessaires à l'analyse de la situation et des besoins du client et rappelle les obligations de protection des renseignements personnels.

### Source — Autorité des marchés financiers : collecte de renseignements et conseil

Le professionnel possède une apparence d'autorité réglementaire. Lorsqu'il affirme devoir obtenir une information, le client peut raisonnablement comprendre que la loi exige exactement ce qu'on lui demande et exactement sous la forme demandée.

Or plusieurs opérations doivent demeurer distinctes : que faut-il légalement vérifier? Que faut-il recueillir? Que faut-il consigner? Que faut-il conserver? Sous quelle forme? Pendant combien de temps? La numérisation de la pièce elle-même est-elle exigée? Qui a décidé de son intégration au système?

Une obligation de vérifier n'est pas nécessairement une obligation de copier. Une obligation de conserver une preuve de vérification n'est pas nécessairement une obligation de conserver une copie numérique intégrale de la pièce. Et une obligation professionnelle de recueillir certains renseignements nécessaires ne constitue pas une autorisation générale d'en recueillir davantage.

### QUI A RENDU CELA OBLIGATOIRE, EN VERTU DE QUOI, ET QUELLE PARTIE EXACTE DE L'EXIGENCE VIENT RÉELLEMENT DE LA LOI?

La réponse peut remonter une chaîne : Loi → Règlement → Organisme de réglementation ou ordre professionnel → Institution → Cabinet → Politique interne → Fournisseur technologique → Configuration du logiciel.

C'est précisément de cette répétition — lorsqu'une exigence institutionnelle, professionnelle ou technologique est perçue comme une obligation légale sans que sa source soit clairement identifiée — que peut naître une culture du consentement non éclairé.

### Un angle mort institutionnel à examiner

L'Office des professions du Québec joue un rôle de surveillance dans le système professionnel. La CAI protège les renseignements personnels. Chaque ordre applique également son propre cadre, auquel peuvent s'ajouter d'autres organismes réglementaires et des obligations fédérales.

Connexion-U ne conclut donc pas, à ce stade, à l'existence d'un « vide juridique » au sens strict. La question est celle d'un possible angle mort transversal : qui vérifie qu'en passant de la loi au règlement, puis à l'ordre, à l'organisation et finalement au logiciel utilisé par le professionnel, une obligation limitée n'est pas devenue une collecte ou une intégration numérique plus étendue que ce que la loi exige?

### L'AUTORITÉ QUI IMPOSE L'EXIGENCE DEVRAIT EN RENDRE LA SOURCE ET LA PORTÉE VISIBLES.

## F. COMMUNICATION À DES TIERS : QUI DÉCIDE?

L'article 18.3 de la Loi sur la protection des renseignements personnels dans le secteur privé permet, sous certaines conditions, la communication sans consentement d'un renseignement à un mandataire ou à un prestataire lorsque cette communication est nécessaire à l'exécution du mandat ou du contrat de service.

Cette possibilité n'est pas une carte blanche. Elle fait apparaître une série de questions que le citoyen voit rarement : qui décide qu'un tiers est nécessaire? Qui décide quels renseignements lui sont nécessaires? Comment la personne peut-elle connaître cette décision? Comment peut-elle savoir où ses renseignements ont circulé? Et que deviennent ses droits lorsque plusieurs acteurs sont impliqués?

**La Liste de vérification devrait identifier non seulement la présence d'un tiers, mais la nécessité qui justifie son intervention, les renseignements auxquels cette intervention lui donne accès, les possibilités de retrait, la porte de sortie et l'alternative non numérique disponible.**

La question devient encore plus importante lorsque les chaînes de fournisseurs ou les infrastructures dépassent les frontières du Québec.

**Source — article 18.3, Loi sur la protection des renseignements personnels dans le secteur privé**

## **G. DESTRUCTION : OBLIGATION ≠ VÉRIFICATION PAR LE CITOYEN**

Le droit québécois prévoit que lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'entreprise doit le détruire ou l'anonymiser selon le cadre applicable, sous réserve notamment des délais de conservation prévus par une loi.

Il faut cependant distinguer une obligation juridique de destruction et la capacité du citoyen de savoir concrètement que cette destruction a eu lieu.

Cette différence devient particulièrement importante lorsqu'un renseignement a circulé entre l'organisation, un prestataire et éventuellement des sous-traitants.

La Liste de vérification pourrait rendre visible : qui détient encore le renseignement; pourquoi; jusqu'à quelle date; et ce qui doit se produire à l'échéance.

**LA TRAÇABILITÉ VÉRIFIABLE DE LA DESTRUCTION CONSTITUE UNE GARANTIE SUPPLÉMENTAIRE PROPOSÉE PAR LA CAMPAGNE.**

**Source — article 23, Loi sur la protection des renseignements personnels dans le secteur privé**

## **H. DÉSABONNEMENT ≠ DESTRUCTION**

Le retrait d'une adresse d'une liste de diffusion et la destruction de tous les renseignements concernant une personne sont deux opérations différentes.

**CESSER UNE COMMUNICATION MARKETING ≠ SUPPRIMER UN COMPTE ≠ RETIRER UN CONSENTEMENT ≠ DÉTRUIRE TOUS LES RENSEIGNEMENTS DÉTENUS**

Cette distinction est particulièrement importante pour l'éducation numérique. Une personne peut croire qu'en cliquant sur « Se désabonner », elle vient de mettre fin à la détention de ses renseignements, alors qu'elle peut n'avoir fait que mettre fin à une utilisation particulière de son adresse.

La Liste devrait donc rendre explicites les conséquences réelles d'un désabonnement, d'une fermeture de compte, d'un retrait applicable et de l'arrivée à échéance d'une période de conservation.

## **I. IDENTITÉ NUMÉRIQUE NATIONALE : FACULTATIVE EN DROIT**

Le droit québécois contient désormais une protection particulièrement importante. L'article 10.3 de la Loi sur le ministère de la Cybersécurité et du Numérique prévoit que l'utilisation de l'identité numérique nationale ne peut être imposée par un organisme public afin de fournir une prestation de services gouvernementale.

Cela établit clairement la non-imposition. Mais cette disposition ne garantit pas, à elle seule, que tous les moyens permettant de ne pas utiliser cette identité — comptoir, service humain ou autre voie analogique — demeureront matériellement accessibles dans le temps.

**FACULTATIF EN DROIT DOIT DEMEURER REFUSABLE EN PRATIQUE.**

Une identité numérique n'est réellement facultative que si la voie permettant de ne pas l'utiliser demeure réellement disponible.

**Source — Loi sur le ministère de la Cybersécurité et du Numérique**

## J. LE PARADOXE DE LA CENTRALISATION

La même loi donne au ministre de la Cybersécurité et du Numérique une mission étendue de coordination de la cybersécurité et de la transformation numérique gouvernementales. Elle lui confie également la gouvernance et la gestion centralisée de l'identité numérique nationale.

La loi institue en outre un registre de l'identité numérique nationale pouvant notamment permettre la conservation sécuritaire de certaines données pour le compte d'organismes publics, leur communication entre organismes et la traçabilité des accès. Elle prévoit également un cadre permettant l'interopérabilité de l'identité numérique nationale avec d'autres infrastructures et systèmes.

La loi prévoit parallèlement des limites à certains usages et maintient la règle de non-imposition de l'identité numérique nationale.

Il n'y a donc pas nécessairement contradiction juridique entre centralisation et non-imposition. Mais leur coexistence soulève une question institutionnelle majeure : qui vérifie, indépendamment de l'autorité chargée de développer, gouverner ou sécuriser l'infrastructure, que son caractère facultatif demeure réel à mesure que cette infrastructure se développe et devient interopérable?

**L'AUTORITÉ QUI CONSTRUIT, GOUVERNE OU SÉCURISE UNE INFRASTRUCTURE NE DEVRAIT PAS ÊTRE LE SEUL REGARD PORTÉ SUR LES EFFETS DE CETTE INFRASTRUCTURE SUR LES DROITS QUI DOIVENT LA LIMITER.**

**Source — Loi sur le ministère de la Cybersécurité et du Numérique**

## K. CE QUE LE DROIT TRANSVERSAL AJOUTERAIT

Notre recherche montre que plusieurs éléments sont déjà protégés, au moins partiellement, par le droit actuel : nécessité; minimisation; finalité; consentement dans les situations où il est requis; accès; rectification; conservation et destruction; encadrement de certaines communications; et non-imposition de l'identité numérique nationale pour obtenir une prestation gouvernementale.

Le droit transversal ne doit pas les remplacer. Il doit permettre :

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

Il rendrait notamment beaucoup plus visibles et exerçables : la justification précise de la nécessité; la distinction entre obligation légale, obligation réglementaire, politique interne et contrainte technologique; les conséquences du refus; la chaîne pertinente des tiers; la durée de conservation; la possibilité effective de retrait ou de dissociation; et la garantie d'une alternative permanente, humaine ou analogique.

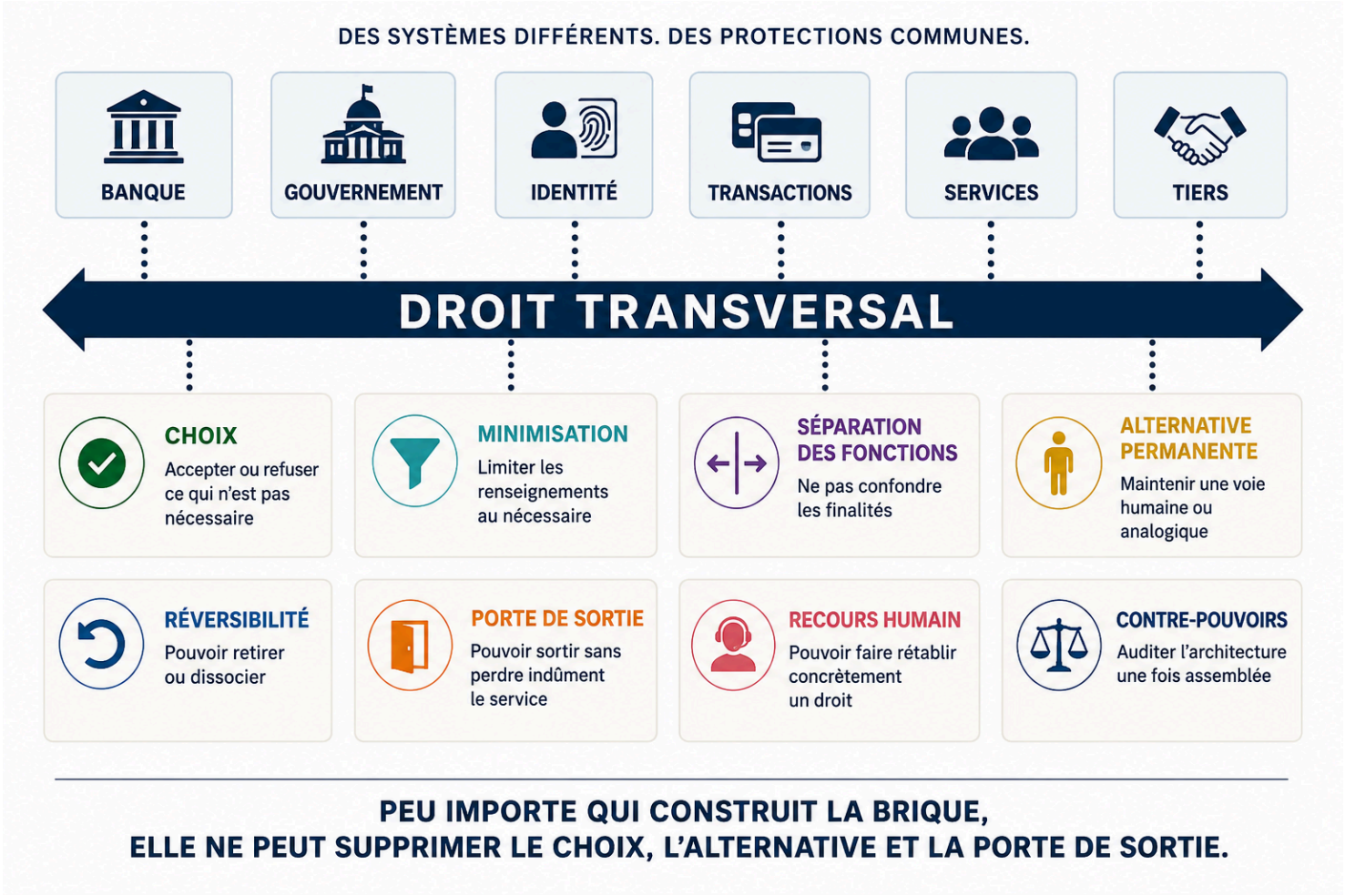
**PROTECTIONS NOUVELLES PROPOSÉES : ÉTIQUETTE DE CONSÉQUENCES NUMÉRIQUES · RÉVERSIBILITÉ · TRAÇABILITÉ DE LA DESTRUCTION · AUDIT INDÉPENDANT · PROTECTION CONTRE L'ATTRITION SILENCIEUSE · DÉROGATION EXPLICITE L. LA LISTE : DU DROIT À L'OUTIL**

La Liste de vérification des conséquences numériques pourrait fonctionner à deux niveaux complémentaires.

### 1. La Liste de vérification institutionnelle

L'organisation devrait rendre visible avant la collecte :

ANNEXE K - DROIT TRANSVERSAL



- RENSEIGNEMENT DEMANDÉ : \_\_\_\_\_
- QUI L'EXIGE : \_\_\_\_\_
- SOURCE : Loi / Règlement / Organisme réglementaire ou ordre / Obligation contractuelle / Politique interne / Configuration technologique
- FINALITÉ : \_\_\_\_\_
- OPÉRATION : Vérifier / Copier / Consigner / Conserver / Numériser / Relier / Communiquer
- TIERS : \_\_\_\_\_
- DURÉE DE CONSERVATION : \_\_\_\_\_
- CONSÉQUENCE DU REFUS : \_\_\_\_\_
- ALTERNATIVE HUMAINE OU ANALOGIQUE : \_\_\_\_\_
- RETRAIT / DISSOCIATION / DESTRUCTION : \_\_\_\_\_
- RECOURS : \_\_\_\_\_

## 2. L'outil citoyen

Le même principe pourrait devenir un outil volontaire permettant à une personne de vérifier, au moment où un renseignement lui est demandé, ce qu'elle doit réellement fournir, pourquoi, sous quelle forme et selon quelle autorité.

### **L'OUTIL DEVRAIT FAIRE LE TRAVAIL QUE LE CITOYEN N'A NI LES MOYENS NI LE TEMPS DE FAIRE DEVANT LE COMPTOIR, LE PROFESSIONNEL OU L'INSTITUTION.**

Une application québécoise d'Étiquette pourrait ainsi devenir un instrument d'éducation, de prévention et de contre- pouvoir.

Son développement pourrait faire l'objet d'un financement public dans un cadre transparent et indépendant. L'expertise citoyenne développée par Connexion-U depuis 2022 pourrait contribuer à sa conception, à son expérimentation et à son déploiement.

Pour préserver la logique même du projet, la gouvernance du contenu de la Liste de vérification des conséquences devrait toutefois être suffisamment indépendante de l'autorité chargée de développer et d'exploiter les infrastructures qu'elle est appelée à examiner.

L'outil pourrait être offert aux citoyens qui souhaitent s'en prévaloir, notamment à partir d'un environnement numérique public accessible, sans en faire une nouvelle obligation numérique.

ANNEXE L - LISTE DE VERIFICATION DES CONSEQUENCES NUMERIQUES

# LISTE DE VÉRIFICATION DES CONSÉQUENCES NUMÉRIQUES

Avant de consentir, savoir à quoi nous consentons.

|  |                                                                                                                                            |                                                                                    |
|--|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
|  | <b>1. RENSEIGNEMENT DEMANDÉ</b><br>Quel renseignement est-il demandé?                                                                      | Permis de conduire                                                                 |
|  | <b>2. QUI L'EXIGE?</b><br>Sur quelle base juridique ou opérationnelle?                                                                     | Loi / règlement / organisme / politique interne / configuration technologique      |
|  | <b>3. FINALITÉ</b><br>Pourquoi ce renseignement est-il demandé?                                                                            |                                                                                    |
|  | <b>4. NÉCESSAIRE AU SERVICE?</b><br>Ce renseignement est-il réellement nécessaire?                                                         | OUI <input type="checkbox"/> NON <input type="checkbox"/><br>Justification : _____ |
|  | <b>5. CONSERVATION</b><br>Est-il seulement vérifié ou également copié et conservé?                                                         |                                                                                    |
|  | <b>6. TIERS</b><br>À qui peut-il être communiqué et pourquoi?                                                                              |                                                                                    |
|  | <b>7. CONSÉQUENCE DU REFUS</b><br>Que se passe-t-il si vous refusez de fournir ce renseignement?                                           | _____                                                                              |
|  | <b>8. ALTERNATIVE HUMAINE OU ANALOGIQUE</b><br>Existe-t-il une alternative humaine ou analogique? Laquelle?                                | _____                                                                              |
|  | <b>9. PORTE DE SORTIE / RÉVERSIBILITÉ</b><br>Comment pouvez-vous retirer ce renseignement ou mettre fin à son utilisation? Comment sortir? | _____                                                                              |

L'organisation doit fournir cette information avant l'acceptation — et non lorsque le citoyen découvre le problème.

## M. LE TEST TRANSVERSAL PROPOSÉ

Dans le nouveau contexte créé par l'assemblage et l'interopérabilité des systèmes, toute nouvelle collecte, infrastructure ou liaison importante devrait pouvoir être soumise à la même séquence :

- Quelle est la finalité?
- Le renseignement est-il nécessaire?
- Qui a décidé qu'il l'était?
- En vertu de quoi?
- L'organisation exige-t-elle ce renseignement, ou son système informatique a-t-il simplement été conçu pour l'exiger?
- Faut-il vérifier le renseignement ou le conserver?
- Faut-il réellement numériser la pièce?
- Faut-il relier ce renseignement à cette identité?
- Faut-il le communiquer? À qui?
- Combien de temps doit-il être conservé?
- Que se passe-t-il ensuite?
- Quelle alternative humaine ou analogique demeure accessible?
- Le refus entraîne-t-il une perte ou une dégradation du service?
- Peut-on retirer ou dissocier ce qui n'est plus nécessaire?
- Comment la destruction peut-elle être vérifiée?
- Qui audite l'architecture une fois les briques assemblées?
- Qui répond démocratiquement de la décision de les relier?

Le droit transversal n'est donc pas une opposition à chaque brique.

**IL CONSTITUE UNE PROTECTION QUI LES TRAVERSE TOUTES.**

**PEU IMPORTE QUI CONSTRUIT LA BRIQUE, ELLE NE PEUT SUPPRIMER LE CHOIX,  
L'ALTERNATIVE ET LA PORTE DE SORTIE — CONDITIONS ESSENTIELLES POUR  
ATTEINDRE RÉELLEMENT LA SOUVERAINETÉ NUMÉRIQUE.**