

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 :

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

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.

CHOIX

Pouvoir accepter ou refuser ce qui n'est pas juridiquement nécessaire.

SÉPARATION DES FONCTIONS

Ne pas relier automatiquement des renseignements simplement parce que la technologie permet de le faire.

RÉVERSIBILITÉ

Pouvoir retirer ou dissocier ce qui n'a plus à être lié ou conservé selon le droit applicable.

RECOURS HUMAIN

Pouvoir joindre une personne capable de rétablir concrètement un droit ou un accès.

MINIMISATION

Ne recueillir et ne conserver que les renseignements nécessaires.

ALTERNATIVE PERMANENTE

Maintenir une voie humaine ou analogique réellement accessible.

PORTE DE SORTIE

Pouvoir sortir d'une architecture sans perdre indûment l'accès au service.

CONTRE-POUVOIRS

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?