

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 questionnement 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

certaines 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 :

- 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.

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.