Cybersécurité et cryptographie post-quantique : Jouer à l’autruche dans un monde quantique!

5 octobre 2026

Auteurs

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

Kiran Younas

Avocate

Les mécanismes cryptographiques qui sécurisent aujourd’hui les transactions, les communications et les signatures numériques pourraient devenir vulnérables avec l’arrivée d’ordinateurs quantiques suffisamment puissants. Pour les entreprises, la question n’est plus seulement d’ordre technologique : elle touche aussi la gouvernance, les contrats, la protection des renseignements et la planification des migrations.

Qu’est-ce que la cryptographie post-quantique?

Pouvez-vous imaginer passer une semaine sans utiliser Internet pour transmettre de l’information sensible? Plus de transactions bancaires, plus de portail permettant de consulter des résultats médicaux, plus d’achats en ligne. Ces activités reposent notamment sur des mécanismes cryptographiques qui :

protègent la confidentialité et l’intégrité de l’information;
authentifient les personnes et les systèmes; et
sécurisent les signatures numériques.

Or, l’avènement d’ordinateurs quantiques suffisamment puissants pourrait compromettre certains de ces mécanismes et, par conséquent, une partie importante de la sécurité sur laquelle repose aujourd’hui notre environnement numérique.

La cryptographie regroupe les techniques qui permettent de protéger la confidentialité et l’intégrité de l’information, d’authentifier les personnes et les systèmes, et de sécuriser les signatures numériques. Elle intervient notamment lorsqu’un navigateur affiche un cadenas, qu’une personne signe électroniquement un document ou qu’une entreprise transmet des données confidentielles. Certains de ces mécanismes reposent sur une paire de clés mathématiquement liées, soit une clé publique et une clé privée. Leur sécurité dépend de problèmes mathématiques que les ordinateurs

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

actuels ne peuvent résoudre dans un délai raisonnable. Un ordinateur quantique suffisamment puissant pourrait toutefois résoudre beaucoup plus rapidement certains de ces problèmes. Des mécanismes largement utilisés, notamment le système RSA et la cryptographie sur courbes elliptiques, n'offriront plus de protection suffisante.

Pourquoi la menace quantique existe-t-elle dès aujourd'hui?

Pour le moment, il n'existe que des prototypes d'ordinateurs quantiques et il demeure difficile de prévoir exactement quand ils deviendront disponibles commercialement ou seront utilisés par certaines grandes entreprises et divers États. Le Centre canadien pour la cybersécurité estime néanmoins qu'un ordinateur quantique capable de représenter une menace pour les mécanismes actuels pourrait être disponible dès 2030, tout en reconnaissant l'incertitude entourant cet échéancier[1]. En août 2024, le National Institute of Standards and Technology des États-Unis a d'ailleurs publié trois premières normes conçues pour résister à cette menace[2]. Pour les organisations, la question n'est donc pas seulement de savoir quand cette menace se matérialisera, mais de déterminer ce qu'elles doivent faire aujourd'hui pour que leurs renseignements et leurs systèmes demeurent sécuritaires dans le futur.

La cryptographie post-quantique désigne les méthodes conçues pour résister aux attaques provenant tant des ordinateurs actuels que de futurs ordinateurs quantiques. D'un point de vue mathématique, des algorithmes résistants existent, mais beaucoup de systèmes informatiques n'en font pas encore usage.

Le risque de « récolter maintenant, déchiffrer plus tard »

On peut résumer la menace la plus pressante par l'expression « récolter maintenant, déchiffrer plus tard ». Un acteur malveillant peut intercepter et conserver aujourd'hui des données chiffrées, puis tenter de les déchiffrer lorsqu'il disposera d'une capacité quantique suffisante. Le risque concerne donc en priorité les renseignements dont la valeur ou la sensibilité persiste pendant plusieurs années, par exemple les secrets commerciaux, les données financières, les renseignements stratégiques et certaines communications privilégiées[3].

L'urgence dépend de la situation technologique propre à chaque organisation. Il faut tenir compte de la durée pendant laquelle les renseignements doivent demeurer confidentiels et du temps nécessaire pour remplacer les mécanismes vulnérables. Selon les meilleures pratiques canadiennes en la matière, certains systèmes ont une durée de vie de 15 à 30 ans et une migration cryptographique peut elle-même prendre plusieurs années[4]. Une organisation peut donc prendre du retard avant même que l'ordinateur quantique menaçant ne soit sur le marché.

Pourquoi les entreprises dépendent-elles de leurs fournisseurs pour la transition?

La plupart des organisations ne développent pas elles-mêmes les solutions cryptographiques de remplacement. Elles dépendent plutôt de leurs fournisseurs de logiciels, de services infonuagiques, d'équipements, de certificats et de cybersécurité.

Cette dépendance ne rend pas la préparation inutile, au contraire. Elle déplace plutôt l'intervention vers la gouvernance, l'approvisionnement et les contrats.

En ce qui concerne les contrats, il est important dès maintenant d'évaluer l'effet de ces risques, notamment la répartition des responsabilités entre les parties contractantes. Idéalement, le contrat de service technologique devra préciser si les risques liés à l'usage de technologies inadéquates du point de vue de la sécurité quantique relèvent du fournisseur ou de son client. Un dialogue dans le cadre duquel les organisations clientes posent les bonnes questions et les fournisseurs technologiques divulguent les limites de leur technologie avec une certaine transparence s'avère donc nécessaire.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

Le gouvernement fédéral a amorcé sa transition vers la cryptographie post-quantique

Le gouvernement fédéral ne traite plus la cryptographie post-quantique comme un simple sujet de recherche. En juin 2025, le Centre canadien pour la cybersécurité a publié une feuille de route pour la migration des systèmes non classifiés du gouvernement du Canada. Ce document prévoit notamment un plan ministériel initial et un premier rapport d'avancement à compter d'avril 2026, la migration des systèmes hautement prioritaires d'ici la fin de 2031 et celle des autres systèmes visés d'ici la fin de 2035[5]. Un avis de mise en œuvre de la Politique sur la sécurité, entré en vigueur en octobre 2025, vise à renforcer ces exigences et impose aux institutions fédérales concernées de démontrer des progrès mesurables[6].

Si ces échéances ne s'appliquent pas directement aux entreprises privées, elles peuvent néanmoins avoir un effet indirect sur les fournisseurs du gouvernement fédéral. Depuis le 1er avril 2026, les contrats fédéraux visés comportant une composante numérique doivent notamment intégrer des clauses favorisant la cryptographie post-quantique et l'agilité cryptographique[7]. Ces mesures confirment qu'une migration ordonnée exige une gouvernance, un inventaire, une priorisation, une planification financière, des politiques d'approvisionnement et une coordination avec les fournisseurs.

De plus, cette orientation dépasse désormais le seul gouvernement fédéral. En septembre 2026, le Canada s'est joint à un appel à l'action du Groupe de travail sur la cybersécurité du G7 invitant les organisations publiques et privées à amorcer une transition progressive fondée sur les risques. Des lignes directrices canadiennes recommandent également aux organisations de commencer leur préparation avant le déploiement de solutions à grande échelle[8].

Quels sont les enjeux juridiques pour les entreprises québécoises?

Aucune loi québécoise n'impose expressément à l'ensemble des entreprises privées d'utiliser un algorithme post-quantique en particulier ou d'effectuer une migration selon l'échéancier fédéral. Le droit québécois formule plutôt des obligations fonctionnelles et technologiquement neutres, lesquelles exigent que l'efficacité des moyens employés soit appréciée dans leur contexte.

Protection des renseignements personnels et mesures de sécurité raisonnables

La *Loi sur la protection des renseignements personnels dans le secteur privé* oblige l'entreprise à prendre des mesures de sécurité raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements. Elle exige également une évaluation des facteurs relatifs à la vie privée lors de certains projets d'acquisition, de développement ou de refonte des systèmes d'information ou de prestation électronique de service qui traitent des renseignements personnels[9]. Pour une organisation qui conserve des renseignements sensibles qui restent pertinents pendant plusieurs années (par exemple des coordonnées bancaires, des numéros d'assurance sociale), le risque quantique pourrait ainsi devenir un facteur pertinent dans l'évaluation du caractère raisonnable des mesures de sécurité actuelles.

Intégrité des documents et confidentialité des transmissions

La *Loi concernant le cadre juridique des technologies de l'information* va dans le même sens en exigeant notamment que l'intégrité d'un document soit maintenue pendant tout son cycle de vie. Par

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

exemple, lorsque les renseignements contenus dans un document sont considérés comme confidentiels en vertu de la loi, l'article 34 exige qu'ils soient protégés par un moyen approprié au mode de transmission[10]. La documentation expliquant le mode de transmission et les mesures prises pour assurer la confidentialité doit également pouvoir être produite en preuve.

Ces dispositions mettent l'accent sur les résultats à préserver, notamment l'intégrité des documents et la confidentialité des renseignements.

Responsabilité civile et état des connaissances

La doctrine québécoise souligne que l'efficacité technique des mesures employées peut devenir juridiquement pertinente[11]. Dans ce contexte, les publications officielles et les normes techniques, sans créer à elles seules une obligation civile, peuvent contribuer à documenter l'état des connaissances, la prévisibilité du risque et les pratiques reconnues[12].

La responsabilité d'une organisation quant aux obligations de protection des données doit être appréciée suivant les règles ordinaires de la responsabilité civile[13]. La question serait notamment de savoir si l'organisation a agi avec prudence et diligence, au moment pertinent, compte tenu :

> des connaissances alors disponibles;
> de la sensibilité des renseignements protégés;
> de la durée de vie de ses systèmes; et
> de l'accessibilité des solutions de remplacement.

Il est possible que l'utilisation d'un mécanisme cryptographique susceptible de devenir vulnérable sous peu constituerait une faute à la lumière des connaissances *actuelles*.

Produits connectés et attentes raisonnables en matière de sécurité

Des considérations semblables pourraient s'appliquer aux fabricants, distributeurs et fournisseurs de produits connectés. Le *Code civil du Québec* tient notamment compte de la sécurité à laquelle une personne peut normalement s'attendre et de l'état des connaissances au moment où le bien a été fabriqué, distribué ou fourni. Dans ce contexte, la capacité raisonnablement attendue d'un produit à recevoir des mises à jour de sécurité pourrait faire partie des circonstances considérées dans l'appréciation d'un éventuel défaut de sécurité[14].

Comment les entreprises peuvent-elles se préparer dès maintenant?

La préparation ne commande pas de remplacer immédiatement tous les mécanismes actuels. Elle vise plutôt à développer une agilité cryptographique, soit la capacité de repérer et de remplacer les mécanismes cryptographiques sans devoir reconstruire entièrement les systèmes qui les utilisent. Le Centre canadien pour la cybersécurité recommande notamment les mesures suivantes[15] :

> **Recenser les usages cryptographiques.** L'inventaire devrait couvrir les systèmes internes et ceux destinés à la clientèle, les certificats, les mécanismes d'authentification, les signatures numériques, les équipements réseau et les services infonuagiques. Une attention particulière devrait être accordée aux systèmes plus anciens, personnalisés ou difficiles à mettre à jour.
> **Établir les priorités.** L'organisation devrait identifier les renseignements qui doivent demeurer confidentiels à long terme et les systèmes dont la modification ou le remplacement nécessitera plusieurs années.
> **Interroger les fournisseurs.** L'organisation devrait obtenir leur feuille de route post-quantique et déterminer si la transition pourra être effectuée au moyen d'une mise à jour ou si elle exigera l'acquisition de nouveaux produits. Les normes utilisées, les périodes de soutien et les conséquences sur l'interopérabilité devraient également être vérifiées.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

Adapter les contrats et l'approvisionnement. Les nouveaux contrats pourraient prévoir, selon le contexte, des exigences relatives aux mises à jour, aux avis de fin de soutien, à l'utilisation de mécanismes normalisés, à la coopération lors de la migration et à la répartition des coûts.

Toutes les organisations ne présentent pas le même degré d'exposition. Une attention immédiate est toutefois requise lorsque l'entreprise conserve des renseignements sensibles pendant plusieurs années, exploite des systèmes difficiles à remplacer ou dépend de fournisseurs dont la stratégie de migration demeure inconnue. Les fournisseurs livreront vraisemblablement les solutions techniques, mais il appartient à chaque organisation de connaître ses besoins, de poser les bonnes questions et de préserver sa capacité de les adopter en temps utile.

Points à retenir :

La menace quantique est déjà présente, même si les ordinateurs quantiques capables de casser certains mécanismes cryptographiques ne sont pas encore largement disponibles.
Le principal risque est celui de **« récolter maintenant, déchiffrer plus tard »** : des données chiffrées aujourd'hui peuvent être conservées et déchiffrées ultérieurement.
Les organisations les plus exposées sont celles qui **conservent des renseignements sensibles pendant plusieurs années**, exploitent des systèmes difficiles à remplacer ou dépendent de fournisseurs dont la stratégie de migration est incertaine.
Au Québec, il n'existe pas d'obligation générale imposant un algorithme post-quantique précis, mais les entreprises demeurent tenues d'adopter des **mesures de sécurité raisonnables**, appréciées selon le contexte et l'état des connaissances.
La préparation passe d'abord par **l'agilité cryptographique** : inventorier les usages, prioriser les systèmes critiques, questionner les fournisseurs et adapter les contrats.

---

1. CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, *Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie* (ITSAP.00.017), février 2025, en ligne : https://www.cyber.gc.ca/fr/orientation/preparez-votre-organisation-menace-pose-informatique-quantique-itsap-00017
2. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, « NIST Releases First 3 Finalized Post-Quantum Encryption Standards », 13 août 2024, en ligne : https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
3. CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, préc., note 1.
4. FORUM CANADIEN POUR LA RÉSILIENCE DES INFRASTRUCTURES NUMÉRIQUES et CANADIAN NATIONAL QUANTUM READINESS WORKING GROUP, *Canadian National Quantum-Readiness Best Practices and Guidelines*, version 04, 10 juillet 2024, p. 3-7, en ligne : https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/documents/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf.
5. CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, *Feuille de route pour la migration vers la cryptographie post-quantique au sein du gouvernement du Canada* (ITSM.40.001), 23 juin 2025, p. 13, en ligne : https://www.cyber.gc.ca/fr/orientation/feuille-route-migration-vers-cryptographie-post-quantique-sein-gouvernement-canada-itsm40001.
6. SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, *La migration du gouvernement du Canada vers la cryptographie post-quantique : Avis de mise en œuvre de la Politique sur la sécurité*, en vigueur depuis le 9 octobre 2025, en ligne : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/politiques-normes/amops/migration-cryptographie-post-quantique-gouvernement-canada.html
7. SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 6, art. 6.3.1.
8. CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, « Appel à l'action du Groupe de travail sur la cybersécurité du G7 concernant la préparation à l'ère post-quantique », 3 septembre 2026, en ligne : https://www.cyber.gc.ca/fr/nouvelles-evenements/appel-laction-groupe-travail-cybersecurite-g7-concernant-preparation-lere-post-quantique; FORUM CANADIEN POUR LA RÉSILIENCE DES INFRASTRUCTURES NUMÉRIQUES et CANADIAN NATIONAL QUANTUM READINESS WORKING GROUP, préc., note 4, sect. 3-5.
9. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1, art. 3.3 et 10.
10. *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1, art. 6 et 34.
11. Éric LABBÉ, « L'efficacité technique comme critère juridique ou la manière dont les lois se technicisent », (2004) 9-2 *Lex Electronica*.
12. Éric LABBÉ, « La multiplicité des normes encadrant le contrat électronique : l'influence de la technologie sur la production des normes », (2004) 9-2 *Lex Electronica*; Charles-Étienne DANIEL, « Coder son propre droit : quand la machine pousse l'humain à énoncer de nouvelles normes de gouvernance », dans *Quand la société fait son droit : la gouvernance de proximité en action*, 2026, EYB2026QSD19, p. 397-432.
13. *Code civil du Québec*, RLRQ, c. CCQ-1991, art. 1457; *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 9, art. 10.
14. *Code civil du Québec,* préc., note 13, art. 1468, 1469 et 1473.

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

15. CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, préc., note 1; CENTRE CANADIEN POUR LA CYBERSÉCURITÉ, *Conseils sur la mise en œuvre de l'agilité cryptographique* (ITSAP.40.018), mai 2022, en ligne : https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-mise-en-oeuvre-de-lagilite-cryptographique-itsap40018

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.