2025

Commission des finances publiques

CFP-020M
C.P. PL 82
Loi concernant
identité numérique nationale

Consultations particulières et auditions publiques sur le projet de loi n° 82, Loi concernant l'identité numérique nationale et modifiant d'autres dispositions

MÉMOIRE

CAPT(RET) STEVE WATERHOUSE, CD

INFOSECSW

Capt (ret) Steve Waterhouse, CD
Expert en cybersécurité, CISSP, C|CISO(A)

Sommaire exécutif

Le projet de loi 82, comme vous savez, précisera certains aspects du projet d'identité numérique pour les citoyens du Québec.

C'est dans un esprit d'interopérabilité qu'il est nécessaire que soit considérée une approche universelle autant dans l'offre de service en matière de cybersécurité envers tous les ministères et organisme, mais aussi envers l'identité numérique. L'Estonie est un cas qui représente bien cette approche recherchée[1]. Pays balte d'une population comparable à la ville de Montréal, a débuté l'aventure de sa transformation numérique en 1994[2] soit au début de leur indépendance de l'URSS, et ont émis des cartes à puce pour l'ensemble de la population en 2002[3], ouvrant la possibilité à la signature numérique et le vote en ligne. Au cours des années suivantes, par l'évolution des technologies, ce pays n'a cessé de constamment améliorer son service pour se trouver aujourd'hui avec la réputation de la société qui a la meilleure pratique d'identité numérique où ses citoyens sont en mesure de voter, effectuer leurs transactions bancaires, valider mariages et transactions immobilières.

En 2014, le cadre de travail eIDAS a été sanctionné en Europe afin de donner la base nécessaire de cette interopérabilité recherchée en Europe. Maintenant, en 2024, la version 2 de ce cadre de travail (eIDAS 2.0[4]) facilitera l'usage de l'identité numérique en Europe tant dans les entreprises privées qu'avec les interactions envers le Gouvernement et autres services publics. Cette merveilleuse aventure me rappelle les premières années d'implantation de la carte à puce au sein du ministère de la Défense nationale (MDN) au début des années 2000 qui avait pour but premier le chiffrement des courriels (jusqu'au niveau Protégé B[5]), authentification lors de connectivité à distance via RPV (VPN), signature numérique (à valeur légale) de documents que pour nommer ceux-ci. Ce système d'Infrastructure à Clé Publique (ICP ou PKI) est toujours en fonction.

Au Canada, le travail de préparation s'est fait depuis plus de 10 ans au gouvernement fédéral, mais aussi dans l'environnement privé, notamment par le Conseil Canadien de l'Identification et l'Authentification Numérique (CCIAN ou DIACC)[6] et la mise en œuvre du cadre de confiance pancanadien (Annexe B) qui a

[1] Estonia e-Identity – https://e-estonia.com/solutions/estonian-e-identity/mobile-id/
[2] This is the story of the world's most advanced digital society – e-Estonia - https://e-estonia.com/story/e
[3] CYBERNETICA - The History of Digital Identity in Estonia – (2020) – https://cyber.ee/resources/news/the-history-of-digital-identity-in-estonia/
[4] The European Digital Identity Regulation – eIDAS 2.0 - (2024) - https://www.european-digital-identity-regulation.com/
[5] Arrêté numéro 2024-05 du ministre de la Cybersécurité et du Numérique en date du 12 décembre 2024 - Modèle de classification de sécurité des données numériques gouvernementales - https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2024F/84711.pdf
[6] CCIAN – DIACC – https://diacc.ca/fr/

mis en commun les parties prenantes de notre société rendant possible qu'un identifiant du Québec sera reconnu ailleurs dans le pays et dans un avenir rapproché avec les commerçants majeurs, ce qu'en Europe a été mis en place il a 15 ans… Le Singapour depuis l'adoption d'une identité numérique nationale en 2003, facilite maintenant l'usage de cette identité à plus de 700 commerçants et services gouvernementaux[7]. Nous sommes très en retard sur l'implantation de ce moyen, mais comment rattraper le temps perdu ? Alors à quant au Canada, y aura-t-il mise en commun de ce genre de projet collectif parmi les 10 provinces et les 3 territoires alors que l'Union européenne compte 27 pays (ou gouvernances) est réalité fonctionnelle et donc sont nettement en avance sur nous.

Tout comme la majorité des concitoyens, je ne veux pas d'un usage dystopique de l'identité numérique ici au Québec. Ces préoccupations sont les mêmes partout autour du monde alors que les abus d'accès à l'information ont été dénombrés à multiples reprises sans trop de conséquences. Comme dans l'étude en 2023 de Comparitech[8], des 35 pays qui ont opté pour l'usage de l'identité numérique via téléphones intelligents, seulement 6 **ne collectent pas de données** à partir de l'appareil. S'il n'y a pas de démonstration / validation franche présentée aux citoyens, l'adoption de ces moyens numérique, aussi prometteurs qu'ils soient, sera vouée à l'échec. Un survol de ces préoccupations courantes est rapporté à l'annexe « A ». Je crois en l'utilité de l'identité numérique, principalement dans la prévention de la fraude par l'identité, aidant les victimes de fuites de données (qui inclus pas mal toute la population à un moment ou un autre), mais pour y arriver, le travail de gagner la confiance des citoyens demeure à mon sens, l'enjeu numéro 1 avant d'aller plus loin.

Merci à nouveau pour cette opportunité d'échanger avec vous. Je suis maintenant disponible à répondre à vos questions.

[7] 8 Countries With the Most Innovative Digital ID Systems – (2025) https://www.beyondencryption.com/blog/countries-most-innovative-digital-id-systems
[8] Digital IDs: 50 countries ranked by digital ID requirements and use – 2024 – https://www.comparitech.com/blog/vpn-privacy/digital-ids-study/

Capt (ret) Steve Waterhouse, CD
Expert en cybersécurité, CISSP

Introduction

C’est un honneur et un privilège de m’adresser à vous sur ce sujet important.

Voici une brève introduction de mes origines. Après 23 ans de service avec les Forces armées canadiennes (R22eR et CIC) et au Ministère de la Défense Nationale (MDN), j'ai eu le privilège d'être parmi les premiers « cyber-soldats » au pays, passant par la gestion des systèmes d'information en réseau de la taille d'un réseau local (LAN - 250 utilisateurs), d’un réseau de campus (CAN - 650 utilisateurs) à celle d'un réseau métropolitain (MAN - plus de 5000 utilisateurs sur plusieurs sites), jusqu’aux premières phases d'intégration de la cybersécurité à titre d’Officier de Sécurité des Systèmes d’Information (OSSI) pendant 13 ans, principalement lors de la renaissance du Collège militaire royal de Saint-Jean (CMRSJ). Plus récemment, outre les divers mandats de consultation avec mon entreprise INFOSECSW, je continue cette mission d’éduquer et former tant les novices que les professionnels des technologies de l’information (TI) et à sensibiliser le public sur la manière d'appliquer les meilleures pratiques de sécurité envers les TI, principalement avec l’Université de Sherbrooke[1] et aussi à titre de chroniqueur en cybersécurité auprès des médias d'information (locaux et nationaux et internationaux), à la participation aux consultation de comités de la Chambre des Communes du Canada ainsi qu’avec l’Assemblée nationale du Québec, mais surtout par la présentation de conférences au pays et ailleurs dans le monde. Depuis 2023, j’agis à titre d’examinateur auprès du comité d’examen indépendant du conseil canadien de l’identité et de l’authentification numériques (CCIAN)[9].

La situation

Dans notre collectivité, nous avons besoin de nous afficher, nous identifier aux autres tout comme les gens font lorsqu’ils naviguent dans le cyber espace. Cependant, le travail de préparation ne fait que s’allonger d’année en année alors que d’autres gouvernances ont réellement fait le choix de numériser les transactions entre les citoyens et les institutions[10]. Entre autres :

1. Le Singapour
2. La Suède
3. L’Estonie
4. La Belgique
5. L’Inde
6. Le Danemark
7. Les Pays-Bas

[9] DIACC – CCIAN – Programme de certification - https://diacc.ca/fr/certification-program-fr/
[10] Beyond Encryption – 8 Countries With the Most Innovative Digital ID Systems – 2025 - https://www.beyondencryption.com/blog/countries-most-innovative-digital-id-systems

8. Le Nigéria

Toujours selon ce rapport de Beyond Encryption, les enjeux qu'ont eu à négocier ces pays pour enfin obtenir ce service, ces moyens d'utiliser l'identité numérique efficacement et avec confiance :

1. **L'infrastructure**

    a. Les gouvernements ont besoin de réseaux robustes capables de gérer une forte demande et de protéger les données.

    b. Ils doivent également s'assurer que les cartes d'identité numériques fonctionnent avec les outils existants, afin que les utilisateurs puissent passer aux solutions numériques. Les systèmes existants peuvent compliquer les choses.

2. **La cybersécurité**

    a. Les cartes d'identité numériques contiennent des données sensibles, ce qui en fait des cibles attrayantes pour les pirates.

    b. Les pays doivent protéger ces systèmes par des mesures de sécurité solides, des mises à jour opportunes et des plans d'intervention clairs en cas de violation. Mais les pirates informatiques évoluent rapidement, d'où la nécessité d'une vigilance constante.

3. **La confiance du public**

    a. Les gens peuvent craindre une utilisation abusive ou une surveillance des données.

    b. Des politiques claires, une communication transparente et des avantages visibles, tels qu'un service plus rapide et une sécurité renforcée, contribuent à instaurer la confiance. Pourtant, les points de vue culturels sur la protection de la vie privée varient d'un pays à l'autre.

4. **La culture numérique**

    a. Pour utiliser les identifiants numériques en toute confiance, les gens ont besoin de compétences techniques de base.

    b. Des formations, des guides utiles et des interfaces faciles à utiliser peuvent permettre à un plus grand nombre de personnes d'en bénéficier.

    c. Pourtant, l'accès universel reste un défi de taille.

5. **Les lois sur la protection des données**

    a. Le respect des règles mondiales en matière de confidentialité des données protège les droits des personnes et rend les identifiants numériques plus fiables.

b. Des lois solides rassurent les utilisateurs en leur montrant que leurs données sont traitées avec soin.

c. Mais l'application de ces lois dépend du système juridique de chaque pays.

De ces enjeux présentés, actuellement, le Québec a la note de 2.5 / 5. La confiance du public est sérieusement à travailler, tout comme augmenter les connaissances numériques par l'intégration (enfin) de programmes scolaires dignes de ce nom, et non en ajouter une couche sur le lot de travail des enseignants actuels aux prises avec ce quotidien endiablé. Puis le 0.5 à la CAI qui doit faire connaître et respecter la loi 25 entre autres pour la protection des données personnelles.

La nécessité du besoin

Je crois que vous trouverez intéressantes les définitions de ce qu'est l'identité numérique au 21e siècle de Montana Kent[11] :

« Comme nous passons de plus en plus de temps dans le monde virtuel, la sécurité et la validité de notre identité numérique deviennent de plus en plus importantes. Le fait de savoir exactement à qui ou à quoi nous avons affaire nous permettra de naviguer en ligne de manière plus sûre. Nous tenons pour acquise la capacité de confirmer l'identité de la partie avec laquelle on interagit lorsque cela se fait face à face.

Pour comprendre l'identité numérique, nous devons d'abord préciser ce que nous voulons dire exactement lorsque nous utilisons le mot **identité**.

Votre identité, dans le contexte de l'interaction avec les autres, contient des identificateurs et des caractéristiques spéciaux qui permettent d'identifier de façon unique qui vous êtes et à vous distinguer des autres. Tout au long de votre vie, vous recueillez des identificateurs et des caractéristiques spéciaux. Certains sont **statiques** et ne changeront jamais, tels que votre date de naissance, alors que d'autres sont **mis à jour** et **changent**, tels que vos titres professionnels.

C'est dans ces cas-ci que l'établissement d'une preuve d'identité devient important, c'est-à-dire la création d'une preuve d'identité sur laquelle d'autres personnes peuvent se fier.

Certains dossiers d'information comprennent des identités **fondamentales**, tandis que d'autres identités sont **contextuelles**, selon le Cadre de confiance pancanadien[MC] (CCP) (Annexe B):

Les **preuves d'identité fondamentale** établissent l'identité des sujets qui sont légalement reconnus comme réels. Elles sont attribuées aux personnes, aux organisations et aux entreprises par certains organismes du secteur public qui sont chargés de créer et de gérer des identités légalement acceptées. Il

[11] ISDE - Série sur la confiance numérique : Première partie | Identité numérique – Montana Kent - Série sur la confiance numérique : Première partie | Identité numérique – 2022 – https://ised-isde.canada.ca/site/justificatifs-numerique/fr/serie-confiance-numerique-premiere-partie-identite-numerique

peut s'agir d'organismes tels que les bureaux du registraire ou de citoyenneté et les agences d'immigration. Un exemple de preuve d'identité fondamentale pourrait être un certificat de naissance ou un article de constitution d'une entreprise.

D'autre part, les **preuves d'identité contextuelle** établissent l'identité des sujets dans des contextes plus spécifiques. Ces types de preuves comprennent des identités qui sont autodélivrées ou administrées à des personnes, des entreprises ou des produits. Elles peuvent être émises par différentes organisations – comme des corporations, des gouvernements et des organisations à but non lucratif.

Des exemples de preuves d'identité contextuelle pourraient comprendre des identifications de la corporation provenant d'un organisme professionnel, l'identité d'une personne sur les médias sociaux ou, dans le cas d'un produit, une identité numérique attribuée par les fabricants.

Bien que l'on pense souvent que les identités ne s'appliquent qu'aux personnes, comme nous pouvons le voir, les identités peuvent également être attribuées aux entreprises et aux organisations. En appliquant ce que nous savons maintenant sur l'établissement de l'identité, il peut y avoir à la fois des informations **fondamentales** qui définissent une entreprise ainsi que des informations **contextuelles** en fonction du travail effectué par cette entreprise ».

Dans l'analyse et considération initiale, la solution de l'application sur téléphone intelligent est favorisée pour question de sa mobilité, facilité de distribution et d'entretien à distance. Le choix d'utiliser une application sur téléphone intelligent s'avère une idée digne du 21e siècle. Selon un sondage de NET Tendance de 2022[12], environ 80% des Québécois auraient un téléphone intelligent avec capacité d'accéder à Internet. Toujours dans l'esprit de garder l'accès à information / aux services numériques, ce projet devra aussi prendre en considération pour l'autre 20% de la population, l'usage de carte à puces comme c'est le cas dans d'autres pays.

Le Bureau du Vérificateur Général (BVG) du Canada en 2024[13] diffusait son rapport avec les difficultés actuelles de financement, mais aussi de faire la consolidation des différents systèmes d'information de tout genre qui ont vu le jour sans trop de contrôle et dont rend difficile une intégration complète vers un système d'identité commune nationale. Cette forme de disparité entre les systèmes d'information du Gouvernement du Québec rend aussi le travail plus difficile pour un déploiement rapide d'une solution d'identité numérique.

[12] NETendances 2022 – Portait numérique des foyers québécois https://transformation-numerique.ulaval.ca/wp-content/uploads/2023/01/netendances-2022-portrait-numerique-des-foyers-quebecois.pdf

[13] Rapport 9. - La validation numérique de l'identité pour accéder aux services – (2024) – https://publications.gc.ca/collections/collection_2024/bvg-oag/FA1-27-2024-1-9-fra.pdf

Recommandations

Dans l'esprit du présent projet de loi 82, je propose que ces recommandations soient considérées pour doter l'administration publique des meilleures pratiques dans l'usage à venir de l'identité numérique:

A. Refaire une Évaluation des Menaces et des Risques (ÉMR) pour un projet d'identité numérique n'est pas seulement une obligation en matière de sécurité : c'est un pilier stratégique pour garantir la protection des utilisateurs, la conformité réglementaire, et la réussite à long terme du projet;

B. Souscrire à la certification du CCIAN est selon moi est essentiel pour tout organisme souhaitant offrir des solutions d'identité numérique fiables, sécurisées et respectueuses des droits des utilisateurs au Canada. Cette certification renforce la confiance, facilite les partenariats, et assure une conformité avec les exigences légales et les meilleures pratiques internationales.

C. Octroyer à tous les citoyens une carte avec puce comme moyen d'identification de base universelle, tel que vue dans les autres pays. Cette carte physique couvre toute la population. La carte d'identité physique à puce doit respecter les critères de l'OACI en matière de lutte contre la contrefaçon et de contrôle d'accès, la norme ISO 29115 (norme d'identification numérique à quatre niveaux d'assurance d'authentification de l'entité), la norme ISO 7816 (norme de carte à puce), la norme ISO 14443 (norme de carte à puce sans contact) et la norme ISO 21188 (norme d'infrastructure à clé publique), ainsi que d'autres normes;

D. Travailler à la pleine interopérabilité de l'identité numérique québécoise dans la province premièrement envers TOUS les services gouvernementaux provinciaux, municipaux et fédéraux, puis envers tous les commerçants qui y souscrivent, puis envers les gouvernances internationales. L'idée est d'assurer que le citoyen québécois ne soit pas pénalisé dans l'accès des biens et services publics, et dans un avenir rapproché, de conclure des transactions d'affaires. Pour appuyer davantage cette approche;

E. La CAI doit augmenter son travail de prévention tant envers la population qu'envers les entreprises, de se faire connaître, faire une plus grande promotion en ce qui concerne les bonnes pratiques de gestion de l'information comme les meilleures pratique au traitement et à la transmission des données sensibles. Cette promotion de meilleures pratiques ne se fait pas qu'à couvert dans un bureau ou derrière quelques publications sur les médias sociaux parce que c'est gratuit, la CAI devrait se montrer plus présente auprès des citoyens lors d'évènement à grand. Et;

F. Octroyé aux services policiers davantage de spécialistes en crime technologique ainsi que les ressources (techniques et financières) nécessaires à aider les enquêteurs dans les nombreuses demandes et croissants d'enquête et d'expertises judiciaires avec la technologie. Sans quoi les délais ne cesseront de s'allonger et les criminels s'en sortiront sans payer de leur crime. Et le citoyen sera mieux desservi alors que c'est actuellement un manque criant, surtout dans les corps policiers municipaux et régionaux.

Les concitoyens se font servir des légendes urbaines quant aux penchants négatifs de l'identité numérique. Voyons comment désamorcer ces croyances.

A. Fuites de données[14]

1. Protéger vos données est devenue une priorité essentielle. Les fuites de données, qui résultent de la divulgation non autorisée d'informations sensibles, représentent un risque majeur. Dans cet article, nous allons vous présenter les différents types de menaces existantes, les bonnes pratiques pour y faire face en cas de crise ainsi que les clés pour vous protéger de ces cyberattaques d'un point de vue individuel et collectif en entreprise.

B. Usurpation d'identité[15]

1. Il est essentiel de protéger votre identité numérique, car une identité compromise peut avoir de graves conséquences, telles que l'usurpation d'identité, la perte financière et l'accès non autorisé à des informations sensibles. Les cybercriminels peuvent utiliser votre identité numérique volée pour ouvrir des cartes de crédit, contracter des prêts ou même commettre des crimes en votre nom. Ils peuvent également accéder à vos comptes et exposer des conversations privées, des photos ou des informations financières.

   Alors que nos vies sont de plus en plus numérisées, les risques associés à la négligence de la protection de l'identité numérique ne cessent de croître. La nature interconnectée de notre monde numérique signifie qu'une faille dans un domaine peut avoir des conséquences considérables sur de nombreux aspects de notre vie. Par exemple, un compte de messagerie électronique compromis peut conduire à un accès non autorisé à de nombreux autres comptes qui utilisent cette messagerie pour se connecter ou récupérer des données.

C. Fraudes[16]
1. Toute information personnelle partagée en ligne court le risque d'être compromise ou volée. Les principales menaces qui pèsent sur votre identité numérique.
    a. Hameçonnage. Une fraudeuse ou un fraudeur vous appelle, vous envoie un texto ou un courriel, ou utilise les médias sociaux pour vous inciter à :
        a. cliquer sur un lien malveillant;
        b. télécharger un maliciel;
        c. transmettre de l'information sensible.

[14] Protéger vos données : Comment prévenir les fuites et assurer leur sécurité – https://cds.thalesgroup.com/fr/hot-topics/proteger-vos-donnees-comment-prevenir-les-fuites-et-assurer-leur-securite
[15] Protecting Your Digital Identity: Strategies and Tools – https://globalcybersecuritynetwork.com/blog/protecting-your-digital-identity-strategies-and-tools/
[16] Comment vous protéger du vol d'identité en ligne (ITSAP.00.033) – https://www.cyber.gc.ca/fr/orientation/comment-vous-proteger-du-vol-didentite-en-ligne-itsap00033

D. L'abus de pouvoir du Gouvernement[17][18]

1. L'identité numérique a le potentiel de jouer un rôle significatif dans la prévention de l'abus de pouvoir des gouvernements, mais cela dépend fortement de son cadre de mise en œuvre, des garanties technologiques et juridiques, ainsi que de la gouvernance qui l'entoure. Voici les aspects principaux à considérer : les systèmes d'identité numérique bien conçus permettent une traçabilité et une transparence des interactions entre citoyens et institutions publiques. Par exemple:

    a. Un vote électronique sécurisé peut réduire le risque de manipulation électorale.
    b. Les registres publics peuvent être accessibles et auditables par des tiers indépendants.

2. Les citoyens pourraient avoir davantage de contrôle sur leurs données personnelles grâce à des mécanismes comme la gestion décentralisée (par blockchain), ce qui limite les abus liés à la surveillance excessive. Les systèmes d'identité numérique peuvent inclure des mécanismes de vérification et de validation des actions des gouvernements, rendant plus difficile la dissimulation de pratiques abusives. L'identité numérique est gérée par un gouvernement sans contrôle externe, cela peut donner à ce dernier un outil puissant pour surveiller, limiter les libertés ou réprimer les dissidents (comme en Chine avec le système de crédit social). Les données collectées dans les systèmes d'identité numérique peuvent être utilisées à mauvais escient pour surveiller les citoyens, rendant plus difficile toute contestation du pouvoir en place. Les systèmes numériques sont sujets aux cyberattaques, aux failles de sécurité et à l'abus par des tiers, ce qui peut compromettre les droits des citoyens et renforcer l'autorité de l'État. Une mauvaise mise en œuvre de l'identité numérique peut marginaliser certaines populations (personnes sans accès à la technologie ou vivant dans des zones rurales).

3. Trucs sur la prévention d'abus de pouvoir :

    a. **Gouvernance multipartite** : L'identité numérique devrait être supervisée par des institutions indépendantes et inclure la participation de la société civile pour éviter toute centralisation abusive.

    b. **Technologies décentralisées** : L'utilisation de systèmes décentralisés, comme la blockchain, peut limiter la concentration du pouvoir et garantir une meilleure transparence.

    c. **Protection des données personnelles** : Des lois robustes (comme le RGPD en Europe) et des outils technologiques pour anonymiser et protéger les données des citoyens sont essentiels.

[17] Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*
[18] World Economic Forum (WEF) : Le rapport " Digital Identity Ecosystems: Unlocking New Value " (2021) https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf

d. **Audit et contrôle externes** : Des audits réguliers et indépendants des systèmes d'identité numérique permettent de détecter et de prévenir les abus.

e. **Recours juridiques** : Les citoyens doivent avoir la possibilité de contester les décisions ou les abus liés à l'utilisation de leur identité numérique.

E. Violation de la vie privée[19]

1. L'identité numérique est un élément essentiel de l'environnement numérique, notamment pour moderniser les services publics. Des initiatives en la matière sont mises en œuvre dans tout le pays pour contribuer à étendre, simplifier et sécuriser l'accès des particuliers aux services publics. Au fur et à mesure que l'écosystème d'identité numérique évolue, les parties prenantes du secteur privé sont appelées à jouer un rôle croissant en tant qu'émettrices et consommatrices de renseignements sur l'identité numérique.

2. Les commissaires à la protection de la vie privée fédérale, provinciale et territoriale et les ombudsmans qui assument une fonction de surveillance dans le domaine au Canada reconnaissent les nombreux avantages potentiels d'une identité numérique sécurisée et respectueuse de la vie privée pour les Canadiens. Le déploiement d'efforts similaires dans d'autres administrations montre que, pour être fiables et largement adoptés, les identités numériques et l'écosystème dans lequel elles sont utilisées doivent répondre à des normes élevées en matière de protection de la vie privée, de sécurité, de transparence et de responsabilité. Sans confiance, les avantages que présente un écosystème d'identité numérique ne se concrétiseront pas.

3. À cette fin, la conception et l'exploitation d'identités numériques respectueuses de la vie privée et d'un écosystème d'identité numérique digne de confiance devraient répondre à la liste non exhaustive suivante de conditions et de propriétés qui devraient également être intégrées à un cadre législatif applicable à la création et à la gestion des identités numériques.

4. En plus d'avoir un écosystème d'identité numérique conforme aux normes et aux meilleures pratiques reconnues à l'échelle internationale, les cadres réglementaires devraient être établis et mis en œuvre de manière à faire respecter le droit à la vie privée et à protéger les données personnelles dans l'écosystème public et privé d'identité numérique. Ces cadres réglementaires devraient être harmonisés partout au Canada pour faciliter l'interopérabilité, tout en respectant les compétences fédérales et provinciales.

F. Surveillance de l'état

1. L'identité numérique, lorsqu'elle est bien conçue, peut jouer un rôle clé dans la prévention de la surveillance étatique excessive. En adoptant des technologies respectueuses de la vie privée et des principes de décentralisation, elle permet aux

[19] Résolution conjointe avec les provinces et territoires – CPVC – Assurer le droit à la vie privée et la transparence dans l'écosystème d'identité numérique au Canada (2022) - https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_220921_02/

individus de protéger leurs informations personnelles tout en limitant la capacité des gouvernements à effectuer une surveillance massive et intrusive.

2. Voici comment l'identité numérique peut prévenir la surveillance étatique :
    a. Décentralisation des données personnelles
    b. Utilisation de technologies anonymisant
    c. Réduction de la centralisation étatique
    d. Transparence et auditabilité
    e. Sécurisation contre l'exploitation abusive des données
    f. Gouvernance basée sur des principes démocratiques
    g. Protection des dissidents et des activistes
    h. Réduction des dépendances technologiques centralisées
    i. Limitation de la surveillance de masse

G. Abus des droits humains[20][21]

1. Pour créer une infrastructure numérique véritablement publique, il est essentiel de donner la priorité aux besoins et aux droits des individus, en particulier ceux qui sont les plus vulnérables à l'exclusion et à la coercition. Pour ce faire, il faut cesser de considérer l'IAP comme une solution purement technique et la comprendre comme un processus social qui doit être régi par des principes d'équité, d'inclusion, de transparence et de responsabilité. La transformation numérique ne devrait jamais être une fin en soi, mais un moyen d'atteindre des objectifs sociaux plus larges. En plaçant les droits de l'homme au centre de l'IAP, nous pouvons faire en sorte que les technologies numériques renforcent les individus et les communautés au lieu d'ancrer les structures de pouvoir et les inégalités existantes.

2. Pour mettre ces principes en pratique, les décideurs politiques devraient suivre les étapes suivantes lors de la conceptualisation, de la conception, de la mise en œuvre, de la maintenance ou de la réforme de l'infrastructure publique numérique (IPN) :
    a. S'engager directement auprès des communautés touchées, de la société civile et d'autres experts pour concevoir des systèmes d'IPN qui répondent aux besoins des personnes les plus exposées, qui sont étroitement adaptés à leur objectif et qui garantissent le respect et la promotion des droits de l'homme.
    b. Veiller à ce que l'IPN soit « public », c'est-à-dire que les autorités - y compris les éventuels partenaires privés - sont responsables devant la population et que la conception et le fonctionnement des systèmes soient transparents.
    c. Intégrer des garanties solides en matière de droits de l'homme dès la phase de conception, comme condition préalable au déploiement de l'IAP à grande échelle. Il s'agit notamment d'adopter et de respecter des normes strictes en matière de

[20] AccessNow - A human rights-centered approach to digital public infrastructure – (2024) - https://www.accessnow.org/guide/digital-public-infrastructure/
[21] Ligue des droits et libertés - Quel respect des droits humains avec l'identité numérique? – (2023) – https://liguedesdroits.ca/quel-respect-des-droits-humains-avec-lidentite-numerique/

respect de la vie privée, de protection des données et de sécurité, et d'offrir des mécanismes efficaces de responsabilisation et de réparation.

d. S'abstenir de rendre les systèmes d'IPN légalement ou pratiquement obligatoires, afin de s'assurer que les individus ont la liberté de choisir d'y participer ou non. Il s'agit notamment de proposer des alternatives analogiques réelles et tangibles aux systèmes numériques.

3. Service québécois d'identité numérique (SQIN)
    a. Un mémoire déposé au Conseil des ministres sur le SQIN en décembre 2021[22] Apporte certaines informations : la « solution d'affaires » vise l'élaboration d'un document d'identité numérique gouvernemental faisant autorité auprès des tiers (public ou privé). Cette identité serait supportée par un portefeuille numérique (application mobile) permettant de conserver des cartes, permis et attestations d'identité divers. Une vérification d'identité « bonifiée » par l'utilisation potentielle de la biométrie, par exemple la reconnaissance faciale, est prévue. Le système aurait un registre doté d'un processus de vérification d'identité de toutes les personnes résidant au Québec.

4. Qu'il s'agisse de discuter en ligne, de partager des contenus sur les réseaux sociaux, de faire des achats sur Internet, d'utiliser des objets connectés ou d'utiliser son smartphone pour lire l'actualité ou effectuer un paiement, toutes ces interactions numériques représentent de nouvelles possibilités d'exercice des droits individuels et collectifs à l'ère numérique[23].

H. Utilisation et abus des données de l'IA[24]

1. Alors que l'IA devient omniprésente dans notre vie quotidienne, s'intégrant de manière transparente dans tous les aspects de nos interactions numériques, le besoin d'une protection solide des données personnelles devient de plus en plus critique. Nous dépassons rapidement la phase initiale d'engouement pour entrer dans une ère où l'IA est la norme tacite, alimentant tout, des assistants de nos smartphones aux systèmes financiers complexes. Cette omniprésence s'accompagne de défis sans précédent en matière de protection de nos identités numériques.

2. Les risques sont multiples, de la collecte de données non autorisées aux techniques d'usurpation d'identité sophistiquées telles que les « deepfakes » et le clonage vocal voit les médias synthétiques. Dans ce contexte, l'établissement et le maintien d'une identité

[22]MÉMOIRE AU CONSEIL DES MINISTRES - Autorisation de la phase d'exécution du projet Identité numérique citoyenne découlant du Programme Service québécois d'identité numérique – (2021) - https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/dossiers-soumis-conseil-ministres/2021-0227_memoire.pdf
[23] OCDE - Droits humains à l'ère numérique - Protéger nos droits à l'ère du numérique - https://www.oecd.org/fr/themes/droits-humains-a-l-ere-numerique.html
[24] Forbes - Stop AI Data Abuse With Decentralized Identity – (2024) - https://www.forbes.com/sites/alastairjohnson/2024/09/12/stop-ai-data-abuse-with-decentralized-identity/

numérique sécurisée et privée n'est pas seulement une question de commodité - elle devient une nécessité pour naviguer en toute sécurité dans le monde piloté par l'IA.

3. La solution réside dans l'adoption de systèmes d'identité décentralisée vérifiée et auto souveraine. Cependant, il est essentiel de comprendre que la simple vérification de l'humanité d'un utilisateur est insuffisante. La véritable sécurité exige une vérification continue par rapport à une identité de confiance existante à chaque point d'interaction, et pas seulement lors de la configuration initiale. Cette approche répond à une préoccupation croissante : la vente d'identités vérifiées sur les marchés noirs, qui reflète le problème de longue date des comptes bancaires compromis utilisés à des fins illicites.

I. État totalitaire[25]

1. L'identité numérique peut être un outil puissant pour prévenir l'autoritarisme numérique en protégeant les droits des citoyens, en favorisant la transparence et en réduisant la centralisation des systèmes. Cependant, son efficacité dépend largement des cadres juridiques, technologiques et éthiques qui l'entourent. Une approche démocratique et multipartite est essentielle pour garantir qu'elle ne devienne pas elle-même un levier d'autoritarisme.

J. La société sans argent liquide[26]

1. Les consommateurs canadiens se tournent de plus en plus vers la technologie sans contact pour effectuer des paiements plus rapides et plus pratiques. Une récente enquête de Moneris auprès des Canadiens a révélé que 67 % des 18-34 ans, 56 % des 35-44 ans, 48 % des 55-64 ans et 49 % des 65 ans et plus préféraient utiliser une carte sans contact pour effectuer leurs achats - la même méthode de paiement que celle utilisée dans les portefeuilles mobiles.

2. L'extension en mai 2016 d'Apple Pay à la prise en charge de toutes les grandes banques canadiennes contribuera également à stimuler l'adoption des portefeuilles mobiles. Parmi les Canadiens âgés de 18 à 34 ans, 46 % ont déclaré qu'ils seraient plus enclins à utiliser un portefeuille mobile s'il était disponible pour le type de carte de crédit qu'ils utilisent, et 47 % ont déclaré qu'ils utiliseraient un portefeuille mobile s'il était disponible pour le type de téléphone qu'ils utilisent - réponses recueillies avant le déploiement complet d'Apple Pay.

3. Interrogés sur les raisons pour lesquelles ils n'utilisent pas de portefeuille mobile, 62 % des Canadiens ont déclaré qu'ils seraient plus enclins à l'utiliser s'ils savaient qu'il était sécurisé. En outre, 50 % des Canadiens ont déclaré qu'ils laisseraient leur portefeuille à la maison s'ils

[25] CSIS.org – Promote and Build: A Strategic Approach to Digital Authoritarianism – (2020) - https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism
[26] Étude MONERIS - Canada pushing toward a cashless society with a 70 per cent drop in cash transactions by 2030 (2016) - https://www.moneris.com/en/about-moneris/news/canada-drop-in-cash-transactions-by-2030

pouvaient stocker toutes leurs cartes de fidélité sur leur téléphone. Les autres raisons pour lesquelles les Canadiens s'accrochent encore à leur portefeuille sont l'impossibilité de recevoir des reçus par courriel (48 %) et de stocker des pièces d'identité (41 %).

4. Comme de plus en plus de consommateurs réalisent que les appareils mobiles offrent une alternative sûre aux portefeuilles physiques grâce à l'authentification biométrique et à d'autres améliorations qui minimisent le risque de fraude, les entreprises devraient intensifier leurs plans pour tirer parti de l'utilisation des appareils mobiles. L'abandon de l'argent liquide est l'occasion pour les entreprises d'offrir une valeur accrue à leurs clients, grâce à des solutions et des applications numériques qui proposent des programmes de récompense et d'autres options de fidélisation, ainsi que des approches de vente omnicanale.

Annexe B
Le cadre de confiance du Conseil Canadien de l'Identification et de l'Authentification Numérique (CCIAN)

À la suite des recommandations du Groupe de travail sur l'examen du système de paiements du gouvernement fédéral, des dirigeants des secteurs public et privé du Canada ont créé le CCIAN en 2012 afin d'élaborer un cadre de confiance pour répondre aux besoins de l'économie numérique.

Le CCIAN s'engage en faveur de l'ouverture, de l'impartialité, de la légitimité et de l'inclusivité, en fournissant le CCP comme un outil qui offre des définitions pratiques des résultats pour vérifier les solutions et réduire les risques d'adoption.

Le Cadre de confiance pancanadien[27] - (CCP) est un cadre d'atténuation des risques composés d'un ensemble de règles, de normes, de spécifications, de règlements et d'orientations qui offre un code de pratique défini de haute qualité et polyvalent pour exploiter une identité numérique fiable et efficace, des titres de compétences et des services de soutien.

CCP : principes et valeurs clés

1. Contribuer à la fiabilité et à l'interopérabilité des capacités de confiance et d'identité numériques des secteurs public et privé tout en donnant la priorité à la conception, à la confidentialité, à la sécurité et à la commodité centrées sur l'utilisateur;

2. Rassembler les meilleures pratiques. Il s'appuie sur les normes, politiques et lignes directrices existantes, en tenant compte des contributions de plusieurs parties prenantes. Le CCIAN s'est engagé à s'aligner sur les cadres pertinents du monde entier pour faciliter l'interopérabilité et l'adoption;

3. Largement applicable, basé sur les résultats, indépendant de la technologie, ouvert et flexible.

Pour les particuliers

1. Améliore la sécurité et la confidentialité tout en offrant un accès pratique et simplifié aux services numériques, réduisant ainsi le risque de vol d'identité et de fraude.
2. Etablit la confiance dans les interactions numériques, permettant aux individus d'utiliser l'identité numérique pour s'engager en toute confiance dans des transactions en ligne et garder le contrôle sur leurs informations personnelles.

Pour les entreprises

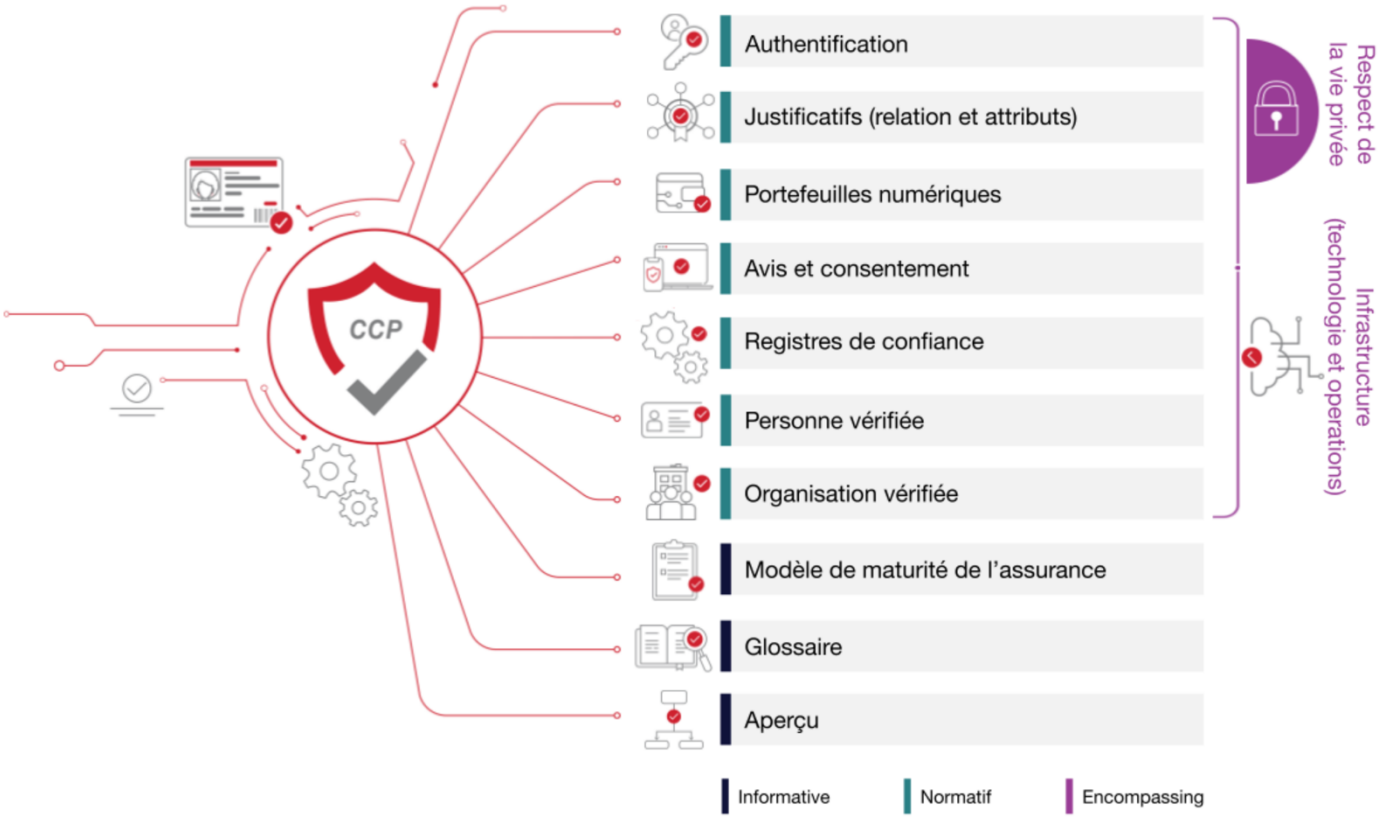
1. Permet de rationaliser les processus d'intégration et d'authentification des clients, de réduire les frictions et d'améliorer l'expérience des utilisateurs.
2. Aide les entreprises à atténuer le risque de fraude et d'accès non autorisé, en protégeant leurs actifs et les données-clients sensibles.
3. Facilite les transactions numériques sécurisées et efficaces, favorisant l'augmentation des opportunités commerciales en ligne et la croissance.

Pour le gouvernement

1. Guide les interactions numériques sécurisées et fiables entre les citoyens et le gouvernement, permettant un accès transparent à divers programmes et services gouvernementaux.
2. Aide les gouvernements à améliorer l'efficacité opérationnelle, à réduire les coûts associés aux processus manuels et à améliorer l'expérience des citoyens et des résidents.

[27] Apperçu du cadre de confiance pancanadien – https://diacc.ca/fr/overview-fr/

Composantes du Cadre de confiance pancanadien[28]
Figure 1



4. D'ailleurs lors de la dernière conférence du CCIAN tenue à Gatineau en 2024[29], la ministre des Affaires étrangères d'Estonie, Mme Nele Leosk, déclara sur l'avancement des travaux di CCIAN :

Cette session résume le développement numérique de l'Estonie au cours des 30 dernières années, en soulignant certains des aspects essentiels de ce voyage. Cette session offrira également un regard sur les nouvelles frontières de l'administration numérique, mais aussi sur la collaboration numérique mondiale en ces temps difficiles.

Nele Leosk
Ministère des Affaires étrangères, ambassadeur itinérant pour les affaires numériques
Département de la diplomatie numérique et cybernétique, Estonie

[28] Cadre de confiance pancanadien « Infrastructure (technologie et opérations) » du CCP recommandation finale V1.2 DIACC / PCTF08 – https://diacc.ca/wp-content/uploads/2024/10/PCTF-Infrastructure-Technology-Operations_Final-Rec-V1.2_Compressed_FRN.pdf
[29] Plénière d'automne 2024 des membres du DIACC – Nov 2024 - https://www.universe.com/events/2024-diacc-member-fall-plenary-tickets-K6BVJ1

Système de crédit social et système de crédit social d'entreprise[30]

Le système de crédit social chinois évalue les individus, les entités et les sociétés en Chine, tandis que le système de crédit social des entreprises ne s'applique qu'aux entreprises.

Le système de crédit social est basé sur de nombreux points de données, de la solvabilité financière aux facteurs sociaux tels que l'honnêteté, le travail acharné et le dévouement à la famille. La Chine dispose de listes noires nationales et régionales basées sur des violations individuelles, et un mauvais score a un impact sur la capacité d'une personne à voyager, à trouver un emploi ou à accéder au crédit.

D'autre part, la notation du système de crédit social des entreprises est basée sur des facteurs liés aux entreprises qui font des affaires ou qui embauchent des employés en Chine, y compris, mais sans s'y limiter, les éléments suivants :

- Le paiement des impôts dans les délais
- Le maintien de licences adéquates
- Respecter les mandats de protection de l'environnement
- Respect des exigences applicables à leur secteur d'activité
- Comportement des partenaires de l'entreprise

Dans le cadre du système de crédit social des entreprises, les entreprises qui ne respectent pas les règles sont placées sur la liste des « irrégularités ». La liste des irrégularités est l'étape qui précède l'inscription sur la liste noire. Les entreprises ont donc encore la possibilité d'améliorer leur score et leur réputation.

Quel est l'objectif du système de crédit social chinois ?

Le système de crédit social chinois vise à s'assurer que les personnes et les entreprises vivant ou opérant en Chine respectent les règles et réglementations en vigueur dans le pays. En imposant des récompenses pour le respect des règles et des pénalités pour le non-respect des règles, le système vise à aller au-delà des codes de conduite suggérés et à appliquer des règles avec des conséquences.

Listes noires et listes rouges dans le système de crédit social chinois

Les listes noires sont fondées sur diverses violations, généralement parce qu'une personne ou une entreprise a commis une violation particulière ou parce que son score de crédit social est faible. Les entreprises ne sont pas automatiquement inscrites sur la liste en cas de manquement à la conformité, mais elles risquent d'être inscrites sur la liste noire si elles ne remédient pas rapidement à ces manquements.

Le système des listes noires est complexe. Les agences d'État et les autorités locales gèrent les listes noires, qui se comptent par centaines dans tout le pays. Une fois inscrit sur une liste noire, il est difficile d'en être retiré. En fait, cela peut prendre jusqu'à deux à cinq ans pour être rayé d'une liste noire.

[30] The Chinese social credit system: What to know as a business owner (2023) - https://velocityglobal.com/resources/blog/chinese-social-credit-system/

Les listes rouges sont l'inverse des listes noires : les personnes et les entreprises dont le crédit social est élevé se retrouvent sur les listes rouges. Les listes rouges sont constituées des membres les plus remarquables de la société du pays ; ces personnes et ces entreprises bénéficient de récompenses telles que l'accès au capital et des approbations accélérées.

How Does the Social Credit System Work?

La Banque populaire de Chine et le gouvernement chinois compilent des données sur les particuliers et les entreprises par le biais de divers supports, notamment les dossiers financiers et gouvernementaux et les plateformes de crédit en ligne.

Une fois collectées, ces données sont ensuite analysées et chaque individu, entreprise et entité gouvernementale reçoit un score de crédit social.

Les personnes ayant un bon score de crédit social sont considérées comme dignes de confiance et bénéficient d'avantages tels qu'une exonération de loyer, des réductions d'impôts, des promotions professionnelles ou des tarifs plus avantageux pour les transports publics.

Ceux qui ont un mauvais score de crédit social sont pénalisés par des refus de prêt, des restrictions de voyage ou même par l'humiliation publique.

Pour les citoyens, les « bonnes » actions peuvent consister à donner du sang ou à faire des dons à des œuvres caritatives, tandis que les « mauvaises » actions peuvent consister à conduire en état d'ébriété.

Pour les entreprises, les « bonnes » actions peuvent consister à effectuer des paiements dans les délais, à faire des dons à des œuvres caritatives ou à obtenir de bonnes critiques de la part des clients et des partenaires commerciaux ; les « mauvaises » actions peuvent être des paiements non effectués, des conflits avec les employés ou le non-respect de la législation locale en matière d'emploi.

Brève histoire du système de crédit social chinois

Le système actuel de crédit social a été mis en place en 2014, mais ses racines remontent à l'époque de Confucius, entre 551 et 479 avant notre ère.

L'idéologie du confucianisme met l'accent sur la contribution de l'individu au bon fonctionnement de la société, en accordant de l'importance au bon caractère. Une autre philosophie, le maoïsme, met l'accent sur l'entraide, tandis que le légalisme insiste sur le respect des lois pour maintenir l'ordre social.

Ces trois écoles de pensée ont influencé la dynastie Qin (221-206 av. J.-C.), au cours de laquelle l'État chinois a mis en place un système d'évaluation méritocratique, même s'il était rudimentaire.

Des systèmes de registres publics permettant de contrôler les comportements des individus sont apparus au 20e siècle avec le « hukou » en 1958, qui enregistraient les ménages et contrôlaient les mouvements domestiques en Chine.

Le système de crédit social actuel a connu ses premières itérations au milieu des années 90, lorsque la Banque populaire de Chine a commencé à partager des informations sur le crédit financier avec les banques commerciales.

Le système de crédit était essentiellement économique jusqu'en 2004, date à laquelle le président Jian Zemin a introduit le système de crédit social. Des projets pilotes régionaux ont été lancés en 2009 et la liste noire a été établie en 2013.

Le gouvernement chinois a adopté le système de crédit social sous sa forme actuelle en 2014.

Avantages du système de crédit social

- Responsabilise les citoyens et les entreprises
- Pourrait accroître la sécurité en Chine
- Motive les citoyens et les entreprises à respecter la loi.

Inconvénients du système de crédit social

- La surveillance vidéo constante en tous lieux est une pratique invasive dans la vie privée.
- Des erreurs de calcul ou de notation de l'algorithme pourraient pénaliser injustement des personnes ou des entreprises.

Comment un système de crédit social affectera-t-il la vie quotidienne des Chinois ?[31]

L'idée est d'utiliser à la fois la carotte et le bâton. Ainsi, une personne ou une entreprise ayant un bon dossier de crédit dans tous les domaines réglementaires devrait bénéficier d'un traitement préférentiel dans ses relations avec le gouvernement, par exemple en étant inscrite sur une liste prioritaire pour l'obtention de subventions. Dans le même temps, les personnes ou les entreprises ayant de mauvais antécédents en matière de crédit seront sanctionnées par la publication de leurs informations, et il leur sera interdit de participer aux appels d'offres des marchés publics, de consommer des produits de luxe et de quitter le pays.

L'année dernière, le gouvernement a publié une liste détaillée des sanctions autorisées. Certaines mesures sont plus controversées ; par exemple, les personnes qui n'ont pas payé les indemnités décidées par le tribunal ne peuvent pas prendre l'avion ou envoyer leurs enfants dans des écoles privées coûteuses, au motif qu'il s'agit d'une consommation de luxe. Le nouveau projet de loi maintient l'engagement que cette liste sera mis à jour régulièrement.

[31] MIT - China just announced a new social credit law. Here's what it means. (2022) – https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean/

Le système fait-il appel à des technologies de pointe, comme l'intelligence artificielle ?

Pour l'essentiel, non. Il s'agit là d'un autre mythe courant concernant le système de crédit social chinois : les gens imaginent que pour suivre les comportements sociaux de plus d'un milliard de personnes, il doit y avoir un puissant algorithme central capable de collecter et de traiter les données.

Mais ce n'est pas le cas. Puisqu'il n'existe pas de système central notant tout le monde, il n'y a même pas besoin d'un algorithme aussi puissant. Les experts du système chinois de crédit social affirment que l'ensemble de l'infrastructure est étonnamment peu technologique. Si les autorités chinoises citent parfois des technologies telles que la blockchain et l'intelligence artificielle lorsqu'elles parlent du système, elles n'expliquent jamais en détail comment ces technologies pourraient être utilisées. Le site web de Credit China n'est rien d'autre qu'une bibliothèque numérisée de bases de données distinctes.

« Il n'existe aucun cas connu où la collecte automatisée de données conduit à l'application automatisée de sanctions sans l'intervention de régulateurs humains », écrit M. Schaefer dans le rapport. Parfois, l'intervention humaine peut être particulièrement primitive, comme dans le cas des « collecteurs d'informations » de Rongcheng, qui se promènent dans le village et notent au stylo les bonnes actions de leurs concitoyens.

Toutefois, au fur et à mesure que le système national se met en place, il semble qu'un élément technologique soit nécessaire, principalement pour mettre en commun les données entre les agences gouvernementales. Si Pékin veut permettre à chaque agence gouvernementale de prendre des décisions en matière d'application de la loi sur la base d'enregistrements collectés par d'autres agences gouvernementales, cela nécessite la mise en place d'une infrastructure massive pour le stockage, l'échange et le traitement des données.

À cette fin, le dernier projet de loi évoque la nécessité d'utiliser « diverses méthodes telles que les méthodes statistiques, la modélisation et la certification sur le terrain » pour effectuer des évaluations de crédit et combiner les données provenant de différentes agences gouvernementales. « Il n'y a qu'un vague soupçon de technologie dans ce projet de loi », déclare M. Daum.

Comment les entreprises technologiques chinoises sont-elles impliquées dans ce système ?

En raison de la faible technicité du système, l'implication des entreprises technologiques chinoises a été marginale. « Les grandes et les petites entreprises technologiques jouent des rôles très différents et adoptent des stratégies très différentes », explique Shazeda Ahmed, chercheuse postdoctorale à l'université de Princeton, qui a passé plusieurs années en Chine à étudier l'implication des entreprises technologiques dans le système de crédit social.

Les petites entreprises, sous contrat avec les autorités municipales ou provinciales, ont largement construit l'infrastructure technique du système, comme les bases de données et les centres de données. D'autre part, les grandes entreprises technologiques, en particulier les plateformes sociales, ont aidé le système à

diffuser son message. Alibaba, par exemple, aide les tribunaux à rendre des décisions de justice grâce aux adresses de livraison qu'elle recueille sur son énorme plateforme de commerce électronique. Douyin, la version chinoise de TikTok, s'est associée à un tribunal local en Chine pour dénoncer publiquement les personnes qui n'ont pas respecté les décisions de justice. Mais ces mastodontes de la technologie ne sont pas vraiment impliqués dans les fonctions essentielles, comme la fourniture de données ou la compilation d'évaluations de crédit.

« Ils ont considéré cela comme une responsabilité civique ou une responsabilité sociale d'entreprise : si vous avez enfreint la loi de cette manière, nous prendrons ces données de la Cour populaire suprême et nous vous punirons sur notre plateforme », explique M. Ahmed.

Certaines entreprises chinoises, comme Ant Group, la branche fintech d'Alibaba, ont également mis au point des produits privés d'évaluation du crédit financier. Mais le résultat, comme le Sesame Credit d'Alibaba, ressemble davantage à un programme de récompenses de fidélité, selon plusieurs universitaires. Étant donné que le score Sesame Credit est principalement calculé sur la base de l'historique des achats et des activités de prêt des utilisateurs sur les propres plateformes d'Alibaba, le score n'est pas suffisamment fiable pour être utilisé par des institutions financières externes et n'a qu'un effet très limité sur les individus.