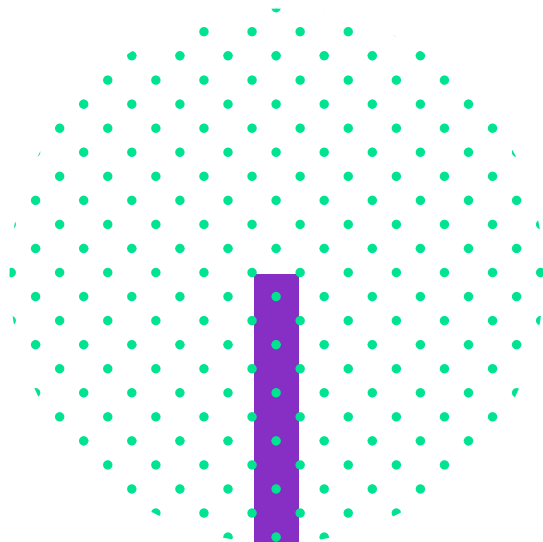




# ASSEMBLÉE NATIONALE DU QUÉBEC


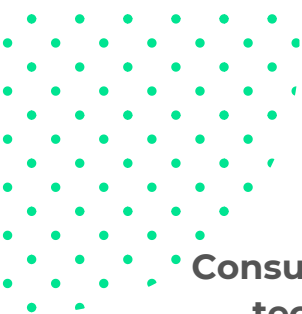
## COMMISSION DES INSTITUTIONS



CHAIRE DE RECHERCHE  
**I.A. RESPONSABLE**  
À L'ÉCHELLE MONDIALE



inclusive  
technology  
lab



# Consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19

Québec, le 14 août 2020

## 1. MÉMOIRE DÉPOSÉ PAR :

### CÉLINE CASTETS-RENARD

Professeure à l'Université d'Ottawa, Faculté de droit civil  
Chaire de Recherche *L'intelligence artificielle responsable à l'échelle mondiale*

Céline Castets-Renard est coresponsable de l'Axe « Relations Internationales, Action Humanitaire Droits Humains » au sein de l'Observatoire International sur les Impacts Sociétaux de l'IA et du Numérique (OBVIA), financé par le FRQSC.

Elle fut professeur d'Université en France pendant 17 ans et est titulaire d'une chaire de recherche Law & AI financé par le gouvernement français au sein de l'*Artificial and Natural Intelligence Toulouse Institute (ANITI)*. Elle fut également chercheuse invitée à la *Fordham Law School (Center of Law and Information Policy)* et *Yale Law School (Internet Society Project)* (2017-2019).

Elle est spécialiste de droit du numérique, droit des données personnelles et vie privée, droit de l'intelligence artificielle dans une perspective comparative de droit européen, américain et canadien.

## 2. RÉSUMÉ DE L'INTERVENTION

Nous souhaitons contribuer au débat sur les outils technologiques de notification des contacts en relevant trois enjeux principaux auquel le gouvernement du Québec doit faire face :

- les risques pour la vie privée et les droits fondamentaux
- le défi de l'utilité et acceptabilité sociale des outils
- au-delà, l'adoption d'un cadre légal sûr et robuste sur l'usage de la technologie par les gouvernements et les entreprises.

Si les deux premiers enjeux portent sur les questions posées aujourd'hui immédiats, ils sont l'occasion de s'interroger plus largement sur le troisième enjeu qui nous paraît essentiel à l'avenir.



### 3. EXPOSÉ GÉNÉRAL

Les outils technologiques de notification des contacts ont été développés un peu partout dans le monde et soulèvent de nombreux enjeux techniques, sociaux et juridiques. Nous nous concentrerons sur les enjeux sociaux et juridiques et mettrons l'accent sur trois d'entre eux.

#### **1ER ENJEU : RISQUES POUR LA VIE PRIVÉE ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**

Bien que la volonté de la plupart des gouvernements démocratiques (au Canada au fédéral et dans les provinces[1], en Europe, en Australie et NZ) soient de tenir compte de la vie privée des citoyens et de protéger leurs renseignements personnels et même si le choix est fait d'adopter les applications les moins intrusives possibles pour la vie privée, par exemple en privilégiant la technologie bluetooth plutôt que GPS le risque zéro n'existe pas et les spécialistes de cybersécurité convergent pour dire qu'il existe des risques de réidentification même dans les choix techniques censés garantir l'anonymat[2], d'autant plus que le déploiement d'une application suppose le recours à une API (*Application Programming Interface*) comme Google ou Apple, ce qui génère encore d'autres vulnérabilité et fuite de renseignements personnels[3].

Pourtant, à la suite de discussions productives et approfondies avec les gouvernements fédéral et ontarien, le Commissariat à la protection de la vie privée du Canada (le Commissariat) et le Commissariat à l'information et à la protection de la vie privée de l'Ontario (CIPVP) ont conclu leur examen de l'application de notification d'exposition Alerte COVID et soutiennent l'utilisation de l'application[4].

L'évaluation sur le plan de la vie privée du gouvernement indique que la *Loi sur la protection des renseignements personnels* fédérale[5] ne s'applique pas à cette initiative puisque, selon ce dernier, l'application Alerte COVID ne recueille pas de renseignements personnels.

Dans son rapport d'examen, le CPVP précise cependant : « Il y a toutefois lieu de prendre note que le gouvernement estime que ses lois en matière de vie privée ne s'appliquent pas à une application considérée dans le monde entier comme ayant une incidence considérable sur la vie privée et qui soulève des préoccupations raisonnables quant à l'avenir des valeurs démocratiques ». « Ici encore, nous faisons face à l'évidence que nos lois doivent être modernisées pour protéger de manière efficace les citoyens canadiens »[6].

[1] <https://www.ipc.on.ca/newsrelease/supporting-public-health-building-public-trust-privacy-principles-for-contact-tracing-and-similar-apps/?lang=fr>.

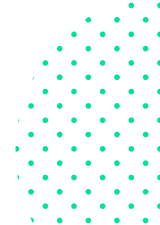
[2] Voir l'audition du professeur Sébastien Gambis devant la Commission des institutions dans le cadre de cette même consultation particulière.

[3] Voir l'audition du professeur Benoît Dupont devant la Commission des institutions dans le cadre de cette même consultation particulière.

[4] <https://www.ipc.on.ca/newsrelease/les-commissaires-federal-et-ontarien-a-la-vie-privee-soutiennent-lutilisation-de-lappli-alerte-covid-sous-reserve-dune-surveillance-continue-de-ses-mesures-de-protection-et/?lang=fr>.

[5] L.R.C. (1985), ch. P-21): <https://laws-lois.justice.gc.ca/fra/Lois/P-21/index.html>.

[6] <https://www.ipc.on.ca/newsrelease/les-commissaires-federal-et-ontarien-a-la-vie-privee-soutiennent-lutilisation-de-lappli-alerte-covid-sous-reserve-dune-surveillance-continue-de-ses-mesures-de-protection-et/?lang=fr>.



**Recommandation 1 : il convient de faire entrer les applications de notification de contacts dans le champ des lois québécoises sur les renseignements personnels**

Nous considérons que même si le risque de réidentification est faible[7], il n'est pas nul. Il conviendrait de considérer que la législation sur la protection des renseignements personnels du Québec s'applique, dès lors que les personnes sont susceptibles d'être identifiées :

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (lois sur l'accès)[8]

Art. 54 : « Dans un document sont personnels les renseignements qui concernent une **personne physique** et permettent de **l'identifier** »

Loi sur la protection des renseignements personnels dans le secteur privé[9]

Art. 2 : Est un renseignement personnel, tout renseignement qui concerne une **personne physique** et **permet de l'identifier**.

Cette interprétation de la loi serait extensive mais correspondrait mieux à la réalité sociale et technique face à des lois adoptées il y a vingt ans. Une réflexion est aussi à mener sur les notions pseudonymisation[10] et anonymisation[11] selon à quoi invite le Commissaire à la protection de la vie privée du Canada (CPVP) dans son Examen des répercussions sur la vie privée de l'application Alerte Covid[12].

[7] Voir l'affirmation du Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIVP) dans ses Recommandations au gouvernement de l'Ontario concernant Alerte COVID : <https://www.ipc.on.ca/wp-content/uploads/2020/07/2020-07-30-ltr-michael-maddock-re-ipc-recommandations-to-the-government-of-ontario-regarding-covid-alert-f.pdf>.

[8] Chapitre A-2.1 : <http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/A-2.1>.

[9] Chapitre P-39.1 : <http://www.legisquebec.gouv.qc.ca/fr/showdoc/cs/P-39.1>.

[10] Art. 4.5 du RGPD : « pseudonymisation », le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

[11] Considérant 26 RGPD : « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable ».

[12] Notre compréhension est que bien que l'identification des utilisateurs soit très improbable, elle n'est pas impossible. Par conséquent, l'utilisation de l'application ne devrait pas être décrite comme étant totalement anonyme. Les données personnelles sont désidentifiées à certaines étapes et les utilisateurs ont des identités pseudonymes à d'autres étapes, mais de telles techniques dans le système ne devraient pas être décrites comme offrant l'anonymat : [https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/urgences-sanitaires/rev\\_covid-app](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/urgences-sanitaires/rev_covid-app).

Il est à noter que d'autres juridictions ont fait le choix d'une autre définition qui permet peut-être d'éclairer le débat de la qualification.

En droit de l'Union européenne, depuis la directive 1995/46/CE du 25 octobre 1995[13], confirmé par le règlement 2016/679/UE (règlement général de protection des données personnelles dit RGPD)[14], de donner une **définition plus large** de la notion de « donnée personnelle » qui recouvre la donnée

Art. 2 de la directive et Art. 4 du RGPD :

« données à caractère personnel » : toute information concernant **une personne physique identifiée ou identifiable** (personne concernée);  
est réputée identifiable **une personne qui peut être identifiée, directement ou indirectement.**

Les données de santé sont en outre des données dites sensibles (art. 9 RGPD).

**Recommandation 2 : il convient de faire un suivi indépendant de la nécessité, proportionnalité et efficacité**

Dans le sens des recommandations du CPVP du Canada et du CIVP de l'Ontario. Parce que l'efficacité de l'application est incertaine, les commissaires ont recommandé que sa mise en œuvre fasse l'objet d'une surveillance étroite, et que l'application soit mise hors service si de nouvelles informations démontrent qu'elle n'est pas ou n'est plus efficace pour atteindre son objectif[15].

[13] <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31995L0046&from=FR>.

[14] <https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR#d1e1438-1-1>.

[15] <https://www.ipc.on.ca/newsrelease/les-commissaires-federal-et-ontarien-a-la-vie-privee-soutiennent-lutilisation-de-lappli-alerte-covid-sous-reserve-dune-surveillance-continue-de-ses-mesures-de-protection-et/?lang=fr>.

[16] Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » : [https://www.cnil.fr/sites/default/files/atoms/files/deliberation\\_du\\_24\\_avril\\_2020\\_portant\\_avis\\_sur\\_un\\_projet\\_dapplication\\_mobile\\_stopcovid.pdf](https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf).

[17] Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid » : <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2020-056-25-mai-2020-avis-projet-decret-application-stopcovid.pdf>.

[18] Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid », JORF n°0131 du 30 mai 2020 : <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041936881&categorieLien=id>.

[19] Décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des solidarités et de la santé : <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000042125452&fastReqId=965192718&fastPos=2>.

Ex. en France l'application Stop Covid a été analysée par la Commission Nationale Informatique et Libertés (CNIL) à deux reprises avant son déploiement. La CNIL a pris deux avis avant le choix de l'application (en avril)[16] et après (en mai)[17] pour un déploiement début juin[18] mais a fait un contrôle et mis en demeure le ministère de la santé le 15 juillet 2020[19].

Il convient de faire une balance des intérêts en présence et reconnaissance de droits fondamentaux à concilier plutôt qu'à opposer : intérêt social vs droits et libertés, santé publique versus vie privée.

Les critères de la balance des intérêts à considérer sont les suivants : nécessité, légitimité, finalité, proportionnalité, efficacité, minimisation des risques.

## **2e enjeu : défi de l'utilité et acceptabilité sociale des outils** **Quels sont les objectifs et la cible ?**

L'efficacité de cette dernière dépendra du taux d'adhésion de la population. Il serait possible à tout moment de désactiver temporairement l'application ou de l'effacer complètement.

Ex. En France : échec à ce jour avec seulement 4% de la population ayant téléchargé l'application Stop Covid sans nécessairement l'utiliser.

L'opportunité d'une telle application n'est-elle pas perdue d'avance ?  
Peut-on réconcilier droit, éthique et efficacité ?

***Recommandation 3 : il convient ne pas considérer que revenir en arrière soit neutre et envisager la fracture numérique.***

Ne pas laisser perdurer une situation inutile et revenir en arrière n'est jamais neutre. Il existe ici un risque social concernant l'appréhension de la technologie : rejet ou banalisation de la technologie

Faire preuve de pédagogie[20] et face au risque social, à la fracture numérique et aux exclusions.

Si le gouvernement du Québec entend se servir de la technologie pour mettre en œuvre ses politiques publiques, il faut mettre en œuvre un grand plan en faveur de l'inclusion numérique.

---

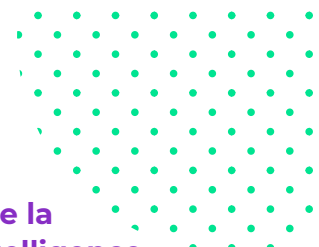
[17] Délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée «StopCovid» : <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2020-056-25-mai-2020-avis-projet-decret-application-stopcovid.pdf>.

[18] Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid », JORF n°0131 du 30 mai 2020 : <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041936881&categorieLien=id>.

[19] Décision n° MED-2020-015 du 15 juillet 2020 mettant en demeure le ministère des solidarités et de la santé : <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000042125452&fastReqId=965192718&fastPos=2>.

[20] <https://observatoire-ia.ulaval.ca/petit-guide-sur-les-enjeux-et-opportunités-des-applications-de-notifications-dexposition-a-la-covid-19>.





### 3e enjeu : besoin d'un cadre légal sûr et robuste pour encadrer l'usage de la technologie par les gouvernements et les entreprises, spécialement l'intelligence artificielle

***Recommandation 4 : il convient de porter une politique ambitieuse en renforçant le cadre légal applicable à la technologie et en particulier à l'intelligence artificielle.***

Le cadre légal est ancien (20 ans) et partiel car il ne couvre pas tous les enjeux. Outre les lois sur les renseignements personnels, la loi concernant le cadre juridique des technologies de l'information (LCJTI)[21] est aussi utile mais l'ensemble est insuffisant.

Le projet de loi 64 va dans le bon sens mais une réflexion plus profonde s'impose car il ne couvrira pas tous les enjeux qui émergent comme la reconnaissance faciale, la police prédictive, les drones, la robotique pour n'en citer que quelques-uns.

Telle est la politique menée par l'Union européenne dans ces Stratégies pour la construction du marché unique numérique[22] et de l'intelligence artificielle[23].

Le Québec est une place forte de l'intelligence artificielle qui doit s'accompagner d'un cadre légal robuste et sûr pour la protection des droits et libertés des individus mais aussi pour promouvoir et sécuriser l'innovation.

Nous remercions la Commission de nous donner cette occasion unique d'ouvrir la discussion et, espérons-le, la coopération entre les députés et les experts indépendants.

---

[21] Chapitre C-1.1 : <http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/C-1.1>.

[22] [https://ec.europa.eu/commission/news/digital-single-market-2018-may-15\\_fr](https://ec.europa.eu/commission/news/digital-single-market-2018-may-15_fr).

[23] Livre blanc Intelligence artificielle : Une approche européenne axée sur l'excellence et la confiance, 19.2.2020 COM(2020) 65 final : [https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020\\_fr.pdf](https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf).