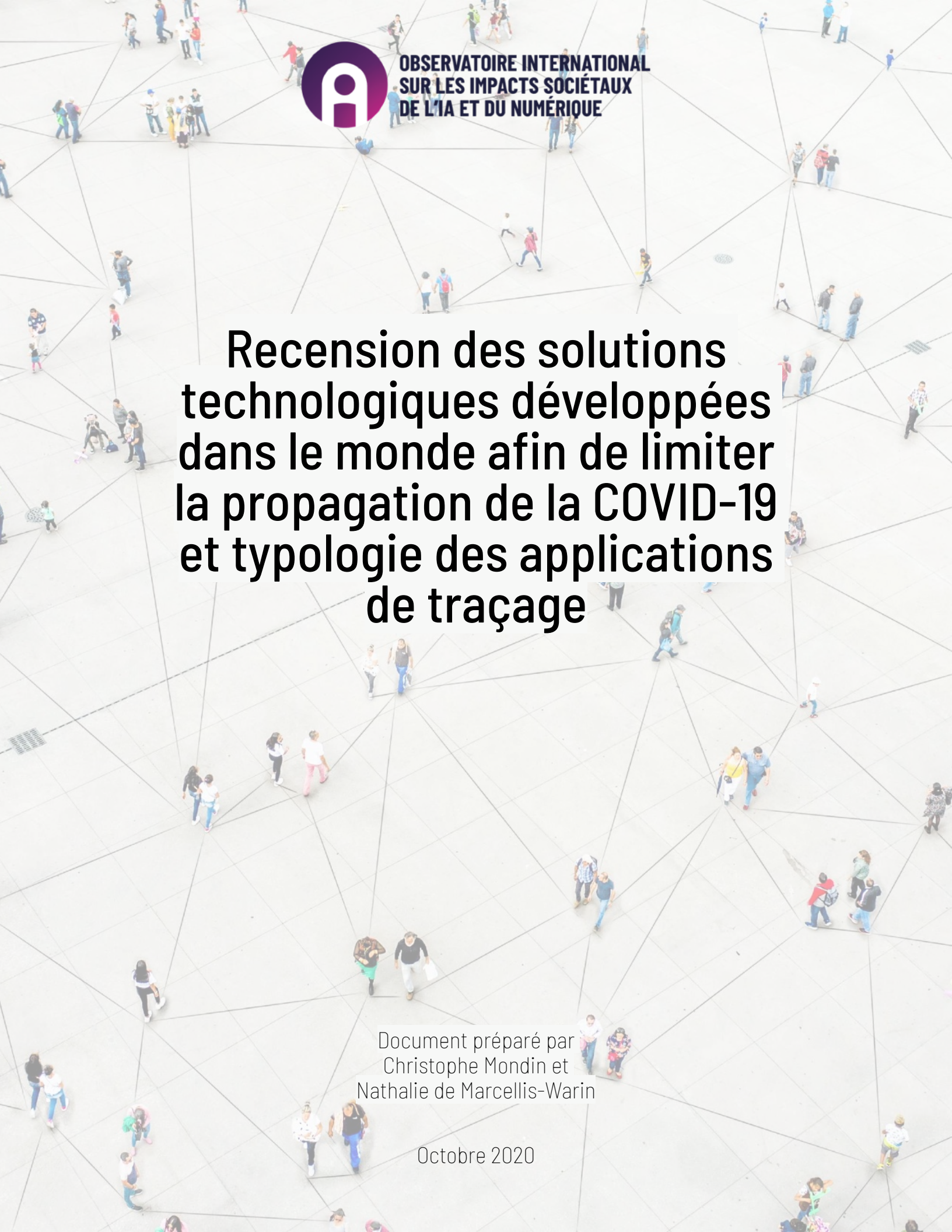

OBSERVATOIRE INTERNATIONAL
SUR LES IMPACTS SOCIÉTAUX
DE L'IA ET DU NUMÉRIQUE

Recension des solutions technologiques développées dans le monde afin de limiter la propagation de la COVID-19 et typologie des applications de traçage

Document préparé par
Christophe Mondin et
Nathalie de Marcellis-Warin

Octobre 2020

Ce document a été préparé sous la direction de la fonction *Veille et enquêtes* de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) dans le cadre des travaux sur les effets des systèmes d'intelligence artificielle et des outils numériques déployés pour lutter contre la propagation de la COVID-19 sur les sociétés soutenues par les Fonds de recherche du Québec (FRQ).

Crédits

Auteur·es

- Christophe Mondin, professionnel de recherche au CIRANO et pour la fonction Veille et enquêtes de l'OBVIA
- Nathalie de Marcellis-Warin, professeure titulaire au Département de mathématiques et de génie industriel, Polytechnique Montréal, présidente-directrice générale du CIRANO et coresponsable de la fonction Veille et enquêtes de l'OBVIA

Contributeur·trices (ordre alphabétique)

- Céline Castets-Renard, professeure titulaire, Faculté de droit, Université d'Ottawa
- Philippe Després, professeur titulaire, Département de physique, génie physique et d'optique, Université Laval, coresponsable de l'axe Santé durable de l'OBVIA
- Pierre-Luc Déziel, professeur agrégé, Faculté de droit, Université Laval, coresponsable de l'axe Droit, cyberjustice et cybersécurité de l'OBVIA
- Sébastien Gambs, professeur agrégé, Département d'informatique, Université du Québec à Montréal
- Lyse Langlois, professeure titulaire, Département des relations industrielles, Université Laval, Directrice générale de l'OBVIA
- Guillaume Macaux, conseiller scientifique, OBVIA

ISBN: 978-2-9818996-9-9

Dépôt légal - Bibliothèque et Archives nationales du Québec, 2020.

Dépôt légal - Bibliothèque et Archives Canada, 2020.

Table des matières

Liste des tableaux

Liste des illustrations

1. Introduction

En réponse à la pandémie de COVID-19 (coronavirus), **la communauté scientifique mondiale, les gouvernements, ainsi qu'une partie de la société civile se sont rapidement mobilisés** pour essayer de ralentir la propagation du virus, protéger la population, sauver des vies et permettre un retour à une vie « normale » avec une reprise des activités économiques le plus rapidement possible.

Les publications scientifiques se sont multipliées et se multiplient encore dans les domaines de la pharmacologie (étude de la structure des protéines affiliées au SARS-CoV-2, études de molécules médicamenteuses), des études cliniques ou encore de l'épidémiologie[1] mais aussi dans les sciences sociales (analyse de scénarios de développement de la pandémie en fonction des choix de politiques publiques de santé, éducation et prévention, impact de la mésinformation, etc.)[2].

Les **gouvernements partout dans le monde ont répondu à la crise sanitaire** en fonction de la vague ou de la courbe des cas infectieux sur leur territoire (amplitude, pente de la courbe), de la capacité de leur système de santé et des moyens sanitaires à leur disposition, mais aussi en fonction de leur situation géographique et politique. Les citoyens ont mis en place diverses initiatives comme du soutien à la population dans le cadre du confinement imposé par leur gouvernement (soutien psychologique, appels téléphoniques de suivi, aide à certaines tâches quotidiennes). De plus, lorsque des données étaient rendues publiques par les gouvernements, des initiatives de visualisation de données ou de cartographie pour suivre la propagation du virus ont aussi vu le jour.

L'ampleur de la crise sanitaire et de ses conséquences socio-économiques directes et indirectes nourrit les craintes exacerbées de la population. L'urgence sanitaire, économique et sociale impose aux autorités la nécessité de trouver des moyens radicaux afin de limiter l'envergure de la pandémie : d'abord en « aplanissant la courbe » des cas d'infection du coronavirus avec des symptômes graves pour ne pas surcharger le système de santé, ensuite en permettant un certain retour à la vie « normale » en limitant les mesures strictes (comme le confinement) qui l'entravent. Au-delà d'assurer la prise en charge des malades, il s'agit pour les gouvernements de trouver les canaux adéquats pour éduquer la population aux bonnes pratiques des gestes barrières, et pour chacun de pouvoir connaître et ainsi limiter son risque d'exposition au virus. Outre les mesures de confinement et d'arrêt des emplois non-essentiels, la capacité de détecter un cas positif pour ensuite rapidement remonter à sa source mais aussi suivre la chaîne de réaction de l'infection semble être la clef de voûte de la stratégie des États pour éviter tout effet domino aux conséquences dévastatrices.

Dans ce contexte, une **multitude de solutions technologiques** s'appuyant sur des outils jusqu'à lors jamais utilisés en contexte de crise sanitaire ont été développées et certaines déjà déployées à

[1] Warin Thierry, 'Global Research on Coronaviruses: An R Package', *Journal of Medical Internet Research, Apr 24* 2020, 22(8):e19615, DOI: 10.2196/19615.

[2] Thiago Carvalho, 'COVID-19 Research in Brief: 6 June to 12 June 2020', *Nature Medicine*, 12 June 2020, https://doi.org/10.1038/d41591-020-00024-y.

travers le monde afin d'aider à lutter contre la propagation du virus. Certaines solutions s'appuient sur l'intelligence artificielle, et de nombreux algorithmes ont été conçus pour répondre aux enjeux de la pandémie[3].

Le risque important d'une propagation exponentielle des cas d'infection du coronavirus a fait planer une ombre funeste dans toutes les sociétés, et avec elle l'urgence d'agir et de rechercher les solutions les plus efficaces, même les plus radicales. Face à une pandémie, le cœur du problème réside dans le domaine de l'épidémiologie, c'est-à-dire l'étude des facteurs et des vecteurs de transmission du virus, mais aussi dans les attitudes individuelles et collectives de la population (confinement, fréquence des petits déplacements, migration, activités et cercles sociaux). Dans un cas comme dans l'autres, des solutions basées sur les nouvelles technologies numériques et l'analyse des données massives (*Big Data*) peuvent être utilisées pour aider à résoudre les problèmes directs et indirects causés par la COVID-19.

En premier lieu, le document fait un tour d'horizon d'un grand nombre de solutions technologiques développées dans le monde en réponse à la pandémie. Cette recension est par la suite axée sur le cas particulier des applications de traçage sur les téléphones intelligents qui visent à limiter les chaînes de contagion, soit par la recherche de contacts (« *contact tracing* ») ou par la localisation (« *position tracking*) » des individus, infectés ou non par le coronavirus. Ensuite, une typologie de ces applications de traçage les présente par grandes catégories et selon leurs caractéristiques principales. Cette analyse descriptive des applications de traçage permet de souligner certains enjeux à prendre en compte lors du choix d'une technologie par rapport à une autre. En conclusion, nous présentons une cartographie qui illustre les différents types de caractéristiques des applications de traçage.

2. Recension des solutions technologiques déployées dans le monde

Afin d'identifier le plus grand nombre de solutions technologiques développées et/ou déployées dans le monde pour lutter contre la propagation du coronavirus, un chantier de veille a été conduit à l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA). Ce chantier a été aussi alimenté par d'autres initiatives semblables à travers le monde, comme par exemple :

[3] 'Mapping the Landscape of Artificial Intelligence Applications against COVID-19 • UN Global Pulse', *UN Global Pulse* (blog), 26 March 2020, https://www.unglobalpulse.org/2020/03/mapping-the-landscape-of-artificial-intelligence-applications-against-covid-19/.

- Le *Covid Tracing Tracker* développé par le journal *MIT Technology Review,* partagé en ligne sous la forme d'un fichier Google Drive[4] [5] [6] ;
- Le répertoire de projets gouvernementaux ou privés utilisant des données personnelles du GDPRhub conçu par l'organisme à but non-lucratif européen NOYB – European Center for Digital Rights[7] ;
- Les travaux parlementaires conduits en France, présentés dans un rapport intitulé « Traçage des données mobiles dans la lutte contre le Covid-19 – Analyse des potentiels et des limites »[8] ;
- Le rapport Digital Solutions for COVID-19 Response - An assessment of digital tools for rapid scale-up for case management and contact tracing publié par l'école de santé publique de l'Université Johns Hopkins aux États-Unis[9].

De plus, la veille a été complétée en recherchant de manière la plus exhaustive possible les solutions technologiques développées et déployées à travers le monde.

2.1. Différents types de solutions technologiques

Sur la période de mars à juin 2020, **plus de 140 solutions technologiques ont été cataloguées dans plus de 50 pays**[10], en particulier des solutions développées pour assurer la détection et le suivi des individus positifs à la COVID-19, ainsi que des **mesures de traçabilité de la population générale ou d'individus en particulier** (*contact tracing* et *position tracking*). Cette liste a été amendée à l'automne, notamment pour y inscrire les dernières solutions déployées dans les provinces canadiennes. Certaines solutions permettent d'évaluer les mouvements de population (par exemple via le bornage téléphonique, les données d'utilisation des cartes bancaires, les applications de conduite). Ces

[4] 'A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them.', MIT Technology Review, n.d., https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

[5] 'MIT TR Covid Tracing Tracker - Articles', n.d., https://www.technologyreview.com/tag/covid-tracing-tracker/.

[6] 'MIT TR Covid Tracing Tracker - Google Sheets', Google Docs, n.d., https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx__zJREoOvFh0nmB-sAqJ1-CjVRSCOw/edit?usp=embed_facebook.

[7] 'Projects Using Personal Data to Combat SARS-CoV-2 - GDPRhub', n.d., 2, https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2#Centralized_contact_tracing_systems.

[8] Mounir Mahjoubi, 'Note parlementaire - Traçage des données mobiles dans la lutte contre le Covid-19 - Analyse des potentiels et des limites' 1 (avril 2020): 44.

[9] Brandon Howard and JH Bloomberg School of Public Health, 'Digital Solutions for COVID-19 Response - An Assessment of Digital Tools for Rapid Scale-up for Case Management and Contact Tracing', Johns Hopkins Bloomberg School of Public Health, n.d., https://www.jhsph.edu/departments/international-health/news/johns-hopkins-researchers-publish-assessment-of-digital-solutions-for-covid-19-response-in-low-and-middle-income-countries.html.

'OBVIA - Solutions technologiques COVID-19', Google Docs, n.d., 19, https://docs.google.com/spreadsheets/d/1zxUr-SfSxwFQFf2I4aKmX5b_jLToGUyfWEM0gcWQmHQ.

solutions technologiques viennent faciliter voire automatiser la tâche des autorités sanitaires dans leur suivi de l'évolution de la pandémie, leur étude des comportements collectifs et individuels, mais surtout dans la recherche des contacts à risque d'un individu infecté par le coronavirus. Lorsqu'une personne reçoit un résultat positif à un test de dépistage de la COVID-19, le but est d'agir au plus vite pour identifier et bloquer la chaîne de transmission, c'est-à-dire la chaîne des contacts physiques à risque (contacts proches, de durée étendue). Cette tâche est habituellement réalisée par des professionnels de la santé, des médecins ou des infirmières, ou bien par des agents du gouvernement représentant les services de santé publique, au moyen d'une enquête qui vise à se remémorer les 14 derniers jours (période d'incubation asymptomatique) et à établir la liste de ces rapprochements à risque. Ensuite, les autorités sanitaires entrent en contact avec les personnes de l'entourage de l'individu infecté et les alertent sur leur situation.

Il existe aussi de nombreuses applications pour téléphones intelligents dont le but est l'auto-évaluation notamment pour déterminer si la personne devrait aller se faire tester. À partir d'un questionnaire à propos des symptômes, de l'état de santé actuel, ou des habitudes de l'utilisateur, une recommandation sur son statut actuel est émise, et des recommandations lui sont transmises par la suite. L'amplitude des données recueillies par ces applications pour établir le niveau de risque de l'utilisateur est assez vaste, allant de quelques questions simples aux renseignements de température ou l'écoute de la toux. Ces applications d'auto-évaluation complètent la tâche des centres d'appels ou des sites internet visant à permettre aux internautes de déterminer, selon leurs symptômes, s'ils devraient aller se faire tester pour la COVID-19 et, si oui, quel est l'endroit le plus proche de leur domicile pour le faire. Une équipe de chercheurs de l'OBVIA s'est d'ailleurs penché sur les différents outils et les sources de données mobilisées pour ces applications de santé et d'auto-évaluation.

D'autres types de solutions technologiques ont été déployées dans le monde pour étudier les mouvements de foule, le suivi des mesures de confinements, etc. Plusieurs exemples peuvent être donnés :

- Certains opérateurs téléphoniques ont mis à disposition les données de bornage téléphonique agrégées et anonymisées de ses utilisateurs. Par exemple, en France, c'est le cas de l'opérateur téléphonique Orange afin d'étudier en partenariat avec l'Institut national de la santé et de la recherche médicale (Inserm) les mouvements de population à la suite des annonces de confinement. Pour l'État, l'enjeu de données fiables et détaillées sur les mouvements de population est double : d'abord à l'échelle nationale et régionale pour adapter par anticipation les capacités médicales, sociales et sécuritaires en fonction du nombre réel de personnes présentes à un endroit donné ; ensuite à une échelle plus locale pour détecter les espaces publics anormalement fréquentés en temps de confinement pour permettre d'adapter localement les réponses sociales, sanitaires et sécuritaires.
- Les appareils photographiques et parfois la reconnaissance faciale ont été utilisés comme outils de contrôler des mesures de confinement et de quarantaine. En Pologne par exemple, la photographie géolocalisée d'un l'utilisateur peut être demandée de manière impromptue

par les autorités sanitaires pour vérifier si la personne est effectivement présente à son domicile.

- Des projets pilotes de télésurveillance (utilisant les caméras de surveillance ou des drones[11]) dans les lieux publics ont été menés par exemple en France pour mesurer en temps réel si les passants se trouvent à une distance suffisante les uns des autres. D'autres projets pilotes de télésurveillance visent, grâce à des algorithmes d'analyse d'images, à contrôler en direct si les individus portent un masque ou non.
- L'accès aux lieux publics comme aux lieux privés est un enjeu majeur pour limiter la propagation du virus et accélérer la reprise des activités normales de la société. Plusieurs types de solutions technologiques ont été développées dans le but de vérifier et d'illustrer le niveau de risque d'infection d'une personne (par exemple via un code couleur) et de suivre les points d'accès voire de limiter l'entrée des individus jugés à risque dans certains lieux (gares, commerces, lieux de travail).

Plusieurs autres moyens techniques, ou combinaison de systèmes, ont aussi été déployés pour poursuivre un même objectif :

- Notification d'exposition pour mesurer les interactions entre les individus, suivre et freiner la propagation du COVID-19 : Bluetooth, localisation (GNSS, type GPS), ultrasons, infrarouges, objets connectés (internet des objets), bornage téléphonique, ou vidéosurveillance ;
- Suivi du déplacement des populations : bornage téléphonique, localisation (GNSS, type GPS), données financières (transactions de cartes bancaires), activités sur les réseaux sociaux (publications pouvant être géolocalisées, contenu des publications) ;
- Contrôle des accès à certains lieux : capteurs et objets connectés, localisation (GNSS, type GPS), QR Codes, vidéosurveillance.

Le niveau de déploiement des solutions technologiques varie grandement à travers le monde. Certaines solutions, applications sur téléphone intelligent ou autres, sont **déjà implantées**, alors que d'autres sont **encore en phase de test**. À chaque fois, l'adhésion de la population, les considérations éthiques en termes de vie privée et de données personnelles, les enjeux d'efficacité et d'acceptabilité sociale jouent un rôle déterminant dans la mise en œuvre effective de ces solutions. Ainsi, la mise en application de certaines solutions a été est **retardée, voire abandonnée** (par exemple en Norvège[12]). Il est par conséquent difficile de donner un état des lieux exact sur le déploiement de ces solutions technologiques, d'autant que les chiffres sur l'utilisation par la population de ces outils ne sont pas toujours publiés.

[11] '« Veuillez respecter les distances de sécurité. » À #Nice, si vous entendez des voix, regardez en l'air. #Drone #SeptAHuit', Twitter, 16 April 2020, https://twitter.com/7a8/status/1250818601621340163.

[12] 'The Norwegian Data Protection Authority Has Imposed a Temporary Ban on Smittestopp Contact Tracing Mobile Application', Datatilsynet, n.d., https://www.datatilsynet.no/en/news/2020/the-norwegian-data-protection-authority-has-imposed-a-temporary-ban-on-smittestopp-contact-tracing-mobile-application/.

2.2. Développement des applications de traçage par pays et à travers le monde

Des solutions technologiques ont été développées à travers le monde, dans certains cas utilisant le même protocole. Singapour est l'un des pays qui a le plus tôt mis en place une application de traçage, *TraceTogether*. La carte ci-dessous permet de visualiser rapidement les pays dans lesquels nous avons pu identifier une ou plusieurs solutions technologiques pour lutter contre la propagation de la COVID-19 :

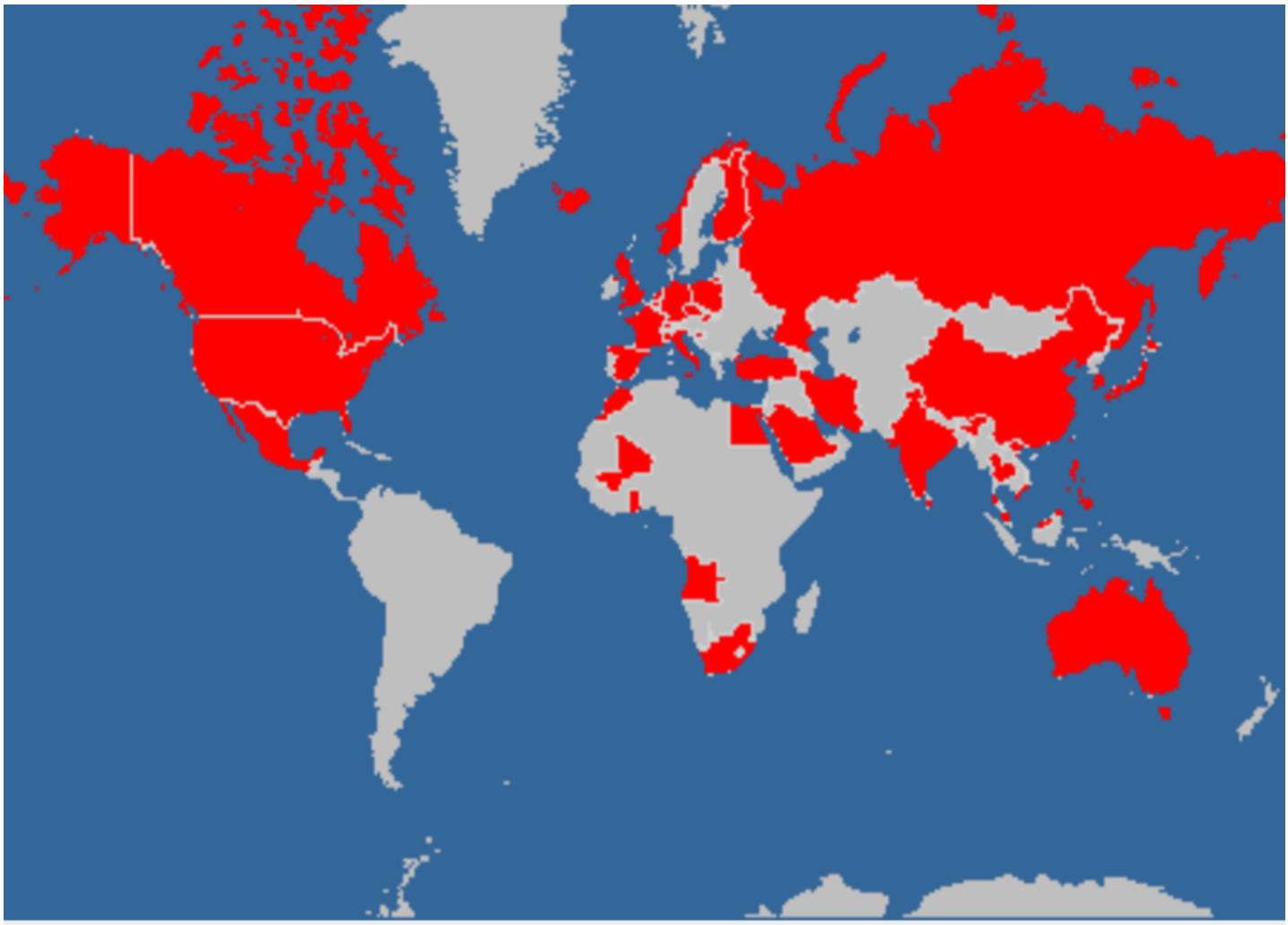

Illustration 1. Pays ayant développé ou fait preuve d'intention de développement d'une solution technologique de type application de traçage dans le contexte de la COVID-19

Les approches et les solutions proposées peuvent être différentes selon les pays ou selon les parties prenantes qui en portent l'initiative (publiques ou privées).

Dans un même pays, plusieurs types de solutions technologiques peuvent être développées. Par exemple, on trouve au Canada plusieurs solutions technologiques avec des finalités différentes qui peuvent être offertes sous la forme d'une application ou d'un site internet (voir le tableau 1).

Tableau 1. Solutions technologiques déployées ou en cours de déploiement au Canada par finalité(s)

Canada/Provinces	Nom	Support(s)	Déploiement	Finalité(s)
Canada	Canada COVID-19	Application et site internet	Mars 2020	Information et auto-évaluation
Colombie-Britannique	COVID-19 BC	Application et site internet	Mars 2020	Information et auto-évaluation
Canada	Alerte COVID/ COVID Alert	Application	Déploiement progressif par provinces	Notification d'exposition (contact)
Canada	COVID Shield (Shopify)	Application	Version originale de COVID Alert (mai 2020)	Notification d'exposition (contact)
Québec	COVI Canada (MILA)	Application	Arrêt développement (juin 2020)	Notification d'exposition (contact, position), évaluation du risque d'exposition, auto-évaluation (symptômes)
Nouveau-Brunswick	SafeContact	Application	Avril 2020 – Probable arrêt du développement	Notification d'exposition (contact, position), évaluation du risque d'exposition, auto-évaluation (symptômes)
Québec	Alerte COVID/ COVID Alert	Application	15 octobre 2020	Notification d'exposition (contact)
Ontario	Alerte COVID/ COVID Alert	Application	31 juillet 2020	Notification d'exposition (contact)
Nouveau-Brunswick	Alerte COVID/ COVID Alert	Application	18 septembre 2020	Notification d'exposition (contact)
Saskatchewan	Alerte COVID/ COVID Alert	Application	18 septembre 2020	Notification d'exposition (contact)
Terre-Neuve-et-Labrador	Alerte COVID/ COVID Alert	Application	3 septembre 2020	Notification d'exposition (contact)
Nouvelle-Ecosse	Alerte COVID/ COVID Alert	Application	15 octobre 2020	Notification d'exposition (contact)
Manitoba	Alerte COVID/ COVID Alert	Application	1er octobre 2020	Notification d'exposition (contact)
Île-du-Prince-Édouard	Alerte COVID/ COVID Alert	Application	8 octobre 2020	Notification d'exposition (contact)
Alberta	Alerte COVID/ COVID Alert	Application	Intention	Notification d'exposition (contact)
Québec	Therappx	Application	Version grand public, mars 2020	Soutien psychologique et/ou émotionnel
Québec	Aller mieux à ma façon	Site internet	Développement en 2019, diffusion pour la pandémie COVID-19 à l'automne 2020	Soutien psychologique et/ou émotionnel

À l'inverse, certaines applications ou protocoles développés à l'origine dans un seul pays sont ensuite proposés de manière *open source* et ensuite déclinés dans d'autres pays ou régions. C'est le cas notamment de l'application TraceTogether, développée par le gouvernement de Singapour, qui a ensuite publié son code source de manière ouverte. Aujourd'hui, le protocole BlueTrace (OpenTrace) est utilisé en Australie pour le déploiement de l'application COVIDSafe, ou en Alberta pour celui de l'application ABTraceTogether.

Sur les 141 solutions identifiées, environ 50 ne sont pas des applications pour téléphones intelligents. La majorité des applications sur téléphones intelligents sont des applications d'information et d'autoévaluation, ou des applications de traçage.

En juin 2020, les chercheurs du pôle santé durable de l'OBVIA ont conduit une veille sur les outils numériques dans la gestion de la pandémie de COVID-19[13] visant à comparer les applications d'information et d'auto-évaluation (auto-diagnostique). Les résultats de ces recherches préliminaires ont été présentés aux décideurs et aux autorités de santé publique provinciaux et fédéraux, et l'ensemble des outils canadiens feront l'objet d'une publication incluant une cartographie au cours de l'automne de l'automne 2020.

2.3. Cas particulier des applications pour téléphones intelligents

Les applications représentent un cas particulier des solutions technologiques déployées dans le monde pour lutter contre la propagation de la COVID-19.

En premier lieu, bien qu'il existe de rares exceptions où le recours à une application de traçage est rendu obligatoire par les autorités (via un décret ou une loi, cette obligation s'accompagnant de mesures contraignantes ou punitives), cette solution technologique est « *opt-in* » (option d'adhésion). Cela signifie que tout individu doit lui-même installer le programme sur son téléphone avant de l'utiliser et donc de véritablement participer à la solution. C'est un élément important à prendre en considération pour les solutions technologiques qui visent à assurer la traçabilité de la population générale ou d'un individu en particulier : celle-ci ne serait pas faite « par défaut », quels qu'en soient les termes. Cette particularité *opt-in* et l'étape d'installation de l'application marquent l'intention de l'utilisateur d'être impliqué dans la solution, et sont donc un moyen de souligner la responsabilité de l'individu, ou en tout cas de lui instiguer la perception d'un sentiment de contrôle. Le coronavirus est un danger pour tous et partout, c'est l'ensemble de la population qui participe d'une manière à la création du risque et s'y expose. Ce risque se révèle avec un certain délai après la contraction de la maladie, et un individu asymptomatique peut être porteur et par conséquent infecter d'autres personnes, en particulier des populations à risque (personnes âgées, nourrissons, individus ayant une santé fragile ou des prédispositions aggravantes). Au même titre que les actions personnelles comme les gestes barrières, le port du masque, ou le respect des règles de distanciation sociale, les applications confèrent à l'utilisateur un rôle de participation active supplémentaire, et par conséquent le responsabilisent.

En second lieu, la distinction des applications comme solution technologique pour lutter contre la propagation du coronavirus tient à son support, le téléphone intelligent. Ce dernier tient une place prépondérante dans nos vies actives et modernes : il peut servir de portefeuille, nous permettre de

[13] Cécile Petitgrand et al., 'OBVIA, Pôle Santé durable - Veille sur les outils numerIA dans la gestion de la pandémie de COVID-19', June 2020, 19, https://observatoire-ia.ulaval.ca/axe/sante-durable/.

surveiller notre budget, être le support de nos loisirs culturels ou vidéoludiques, être lié à notre carte de transport en commun, ou être un socle de nos relations sociales et amoureuses. Pour beaucoup, le téléphone intelligent est aujourd'hui l'incarnation de l'objet personnel ultime, voire intime, à la limite de l'extension de la personne. Ce caractère identitaire du téléphone intelligent se retrouve dans de nombreuses applications et fonctionnalités : publications de messages géolocalisés, calculs de trajets et suivi des déplacements, enregistrement de certaines interactions ou de certaines activités, profils sur les réseaux sociaux.

Ces attributs en font un support idéal pour les solutions technologiques déployées pour lutter contre le coronavirus. Additionnellement, les applications sur téléphone intelligent sont en apparence très faciles d'accès et d'utilisation (à condition de posséder un tel appareil). Évidemment, des enjeux vont de pair avec ces caractéristiques : consentement éclairé, de surveillance via les données massives et la géolocalisation, de littératie numérique, ou des principes de fonctionnement de base des algorithmes et de l'intelligence artificielle utilisant les données personnelles. L'ensemble de ces technologies est né récemment et se transforme à mesure qu'elles se déploient, et bien souvent la population garde une attitude relativement ingénue quant à leur utilisation. Face au rythme effréné d'évolution et d'emploi des technologies accessibles sur les téléphones intelligents, les utilisateurs comme les autorités régulatrices ont de la peine à faire preuve du recul nécessaire, si tant est qu'il soit possible d'analyser avec introspection les tendances et les évènements se déroulant aujourd'hui sous nos yeux.

2.4. Spécificités des applications de traçage

Les applications de traçage se déclinent en deux principales familles :

- Les applications de traçage de contact *:* la recherche de contact a lieu entre deux utilisateurs de l'application. Le but est, lorsqu'une personne est testée positive à la COVID-19, d'avoir un historique des rapprochements physiques « à risque » avec d'autres personnes, ayant elles aussi installé l'application.
- Les applications de suivi de position : le pistage de la position et/ou des déplacements de l'utilisateur. L'objectif est, lorsqu'une personne est testée positive au COVID-19, de pouvoir s'assurer qu'elle ne met pas d'autres personnes en danger d'infection. Ces applications sont utilisées dans l'exécution de mesures de quarantaine strictes, parfois associées à des mesures de coercition. Une déclinaison des applications de suivi de position peut être vouée à interdire ou autoriser l'accès à un lieu en fonction de l'état de santé de l'utilisateur de l'application, voire d'un calcul de la probabilité – ou du risque – d'être infecté.

Toute situation de crise est propice à la diffusion de préjugés et de stéréotypes, et le déploiement des applications de notification d'exposition soulève des enjeux de stigmatisation et de discrimination. Une personne malade ou supposément malade peut être victime d'ostracisme, et des lieux ou des

communautés entières peuvent subir le même sort en étant l'objet de méfiance et de rejet, justifiés par l'utilisation de ces outils et des renseignements qu'ils diffusent[14][15].

Avec la collecte de données qui peuvent être géolocalisées, des cartes précises peuvent être dressées pour faire un bilan de l'évolution de la maladie et délimiter des zones à risque. C'est une extension des cartes qui peuvent être présentées en fonction du nombre de cas recensés par les autorités ou du taux d'occupation des lits dans les hôpitaux. Des procédés de cartographie et de géorepérage (gardiennage virtuel, *geofencing*) peuvent être développés pour alerter les utilisateurs voire contrôler et interdire certaines zones (quartier, lieu public, magasin).

Cet environnement de crainte causé par la pandémie peut aussi marginaliser les personnes qui décident de ne pas d'utiliser une application de traçage, ou ne peuvent pas utiliser cette solution (par exemple s'ils n'ont pas de téléphone intelligent, si la fonctionnalité Bluetooth est défectueuse, si leur modèle est trop ancien[16], etc.). L'absence de l'application de traçage crée de l'incertitude, et pourrait être perçu comme un aveu d'infectiosité. Certains établissements publics, des lieux de restauration, ou encore des lieux de travail pourraient, animés de bonnes intentions, vouloir imposer l'utilisation de ce type d'application avant d'y accéder et transformeraient de facto une application volontaire en application obligatoire.

Sous l'égide de l'axe de recherche Droit, cyberjustice et cybersécurité de l'OBVIA, une équipe de chercheurs a publié au début de l'été 2020 un guide[17] à l'intention des utilisateurs potentiels des applications de traçage. Sous forme de foire aux questions, c'est un document didactique qui vise à expliquer les notions à prendre en considération lorsqu'une personne songe à installer et faire usage de ce type de solution technologique.

Bien que les applications de traçage n'aient jamais (ou du moins pas encore) pris une place centrale dans les moyens effectivement employés par les autorités sanitaires pour contrer activement la pandémie, elles ont cependant rapidement pris une place prépondérante dans les débats et ont d'abord été présentées comme une pièce maîtresse de l'arsenal technologique à déployer. Plusieurs arguments pesaient en faveur de cette solution et semblaient les imposer comme des outils presque indispensables à diffuser dans les pays ayant atteint un certain seuil de développement numérique : une application de traçage est un outil technologique, qui peut – relativement – facilement atteindre l'ensemble de la population avec de grandes utilités et efficacités théoriques puisqu'elle permet à la fois d'agir précisément à l'échelle individuelle en limitant la propagation du virus tout en renseignant la santé publique sur la situation et les modalités de transmission de la maladie en quasi temps réel. Dès les annonces d'intention de développement et de déploiement de cette solution, les nombreux

[14] 'Efficacité et enjeux sociétaux des apps de traçage de contacts', Observatoire international sur les impacts sociétaux de l'IA et du numérique, 27 April 2020, https://observatoire-ia.ulaval.ca/3674/.

[15] 'Attention à la surveillance technologique généralisée', Le Devoir, n.d., https://www.ledevoir.com/opinion/idees/577688/attention-a-la-surveillance-technologique-generalisee.

[16] Reed Albergotti, 'Apple and Google Launch Coronavirus Exposure Software', *Washington Post*, n.d., https://www.washingtonpost.com/technology/2020/05/20/apple-google-api-launch/.

[17] 'Petit guide sur les enjeux et opportunités des applications de notifications d'exposition à la COVID-19', Observatoire international sur les impacts sociétaux de l'IA et du numérique, n.d., https://observatoire-ia.ulaval.ca/qa_covid/.

enjeux allant de pair avec les applications de traçage ont été soulignés, et l'attention a été attirée sur les insuffisances et limites de ces solutions : l'efficacité ou l'utilité relative (par rapport à d'autres initiatives), les défis du recrutement de la population (masse critique d'utilisation), l'acceptabilité sociale, la sécurité et la confidentialité des données sensibles, etc. Singapour est l'un des pays qui a le plus tôt mis en service une application de traçage, TraceTogether, dont le développeur principal remettra en cause au bout de quelques semaines ses avantages et ses impacts dans l'article « *Automated Contact Tracing Is Not A Coronavirus Panacea* » [18]. Le discours entourant le développement des applications de notification d'exposition a beaucoup évolué au long du printemps et de l'été 2020, à mesure que les différentes vagues de la pandémie déferlaient autour du monde et que les pouvoirs publics, qui n'étaient plus pris de cours, s'adaptaient. L'engouement pour ce type de solution technologique s'est tari d'abord parce que les discussions publiques ont continué de souligner les problématiques éthiques inhérentes au déploiement de ces applications, ensuite parce que l'adoption précoce de ce type d'application de traçage par plusieurs nations dans le monde présentait des résultats au mieux mitigés.

Au printemps et au cours de l'été 2020, de nombreuses initiatives[19] à travers le monde ont souligné les implications du déploiement des applications de traçage et ont mis en exergue les enjeux éthiques, juridiques et sociétaux de ces solutions, et ont mis en perspectives ces enjeux par rapport à l'utilité et l'efficacité présumées des applications de traçage. Ces réflexions ont été particulièrement prolifiques au Canada au Québec. Au niveau fédéral, le Commissariat à la protection de la vie privée (CPVP) a publié deux documents : un document d'orientation[20] produit en mars 2020, et un cadre d'évaluation[21] des initiatives pouvant porter atteinte à la vie privée produit en avril 2020. Au niveau provincial, de très nombreux travaux ont vu le jour au Québec. La Commission d'accès à l'information (CAI) a publié un document de réflexion[22] concernant le recours à certaines technologies (mai 2020), dont les applications de notifications d'exposition. Ce document visait d'avantage l'harmonisation entre les efforts et mesures contre la propagation du COVID-19 d'un côté, et la reprise de l'activité économique de l'autre. La Commission de l'éthique en science et en technologie (CEST)

[18] Jason Bay, 'Automated Contact Tracing Is Not a Coronavirus Panacea', Medium, 20 April 2020, https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98.

[19] 'ACLU White Paper: The Limits of Location Tracking in an Epidemic', American Civil Liberties Union, n.d., https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic.

[20] Commissariat à la protection de la vie privée du Canada, 'La protection de la vie privée et l'éclosion de la COVID-19', 20 March 2020, 19, 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/gd_covid_202003/.

[21] Commissariat à la protection de la vie privée du Canada, 'Cadre pour l'évaluation par le gouvernement du Canada des initiatives en réponse à la COVID-19 ayant une incidence importante sur la vie privée', 17 April 2020, 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/fw_covid/.

[22] CAI, 'Pandémie, Vie Privée et Protection Des Renseignements Personnels', May 2020, https://www.cai.gouv.qc.ca/documents/CAI_document-reflexion_PRP_COVID-19_FR.pdf.

a constitué un comité spécial[23], publié deux rapports[24] sur les facteurs d'acceptabilité éthique du recours aux applications intégrant des systèmes d'intelligence artificielle pour contrôler la propagation de la COVID-19. Le rapport final[25] a été publié le 12 août 2020. La CEST a par ailleurs travaillé conjointement avec le comité d'éthique de santé publique pour produire un cadre de réflexion[26] sur les enjeux éthiques liés à la pandémie. Enfin, le Centre de recherche en éthique (CRÉ) a publié une liste des sept principaux enjeux éthiques[27] soulevés par le déploiement des applications de notification d'exposition. La crise sanitaire a contribué à démocratiser les enjeux importants du virage numérique : la définition de donnée personnelle, la protection de l'anonymat, et la confidentialité des données ont été au cœur des discussions, et le gouvernement québécois a même lancé une consultation publique en ligne au sujet des applications de notification d'exposition. Tous ces éléments, ainsi que des questions plus précises concernant par exemple la souveraineté des données, ont aussi été abordés lors de délibérations publiques à l'assemblée nationale du Québec en août.

Le vif engouement initial suscité par les applications de traçage et le nombre important de ces outils développés et d'ores-et-déjà implémentés à travers le monde offrent l'opportunité de comparer ces solutions entre elles selon différents critères, d'en analyser les différences et les points communs. Les multiples enjeux promptement soulevés et débattus font de ces applications un sujet important d'étude, et pour mieux comprendre les implications possibles de leur usage, la compréhension de cette technologie est une étape nécessaire. La suite du document présente une typologie des applications de traçage et a pour vocation de pouvoir naviguer et saisir les différentes options, déclinaisons, et principes de cette technologie.

3. Typologie des applications de traçage

La recension des 141 solutions technologiques déployées dans le monde a permis d'identifier **presque 100 applications de traçage**[28] disponibles (à des stades de développement et des niveaux d'utilisation variables).

[23] CEST, 'Comité spécial - Enjeux éthiques liés à la pandémie de COVID-19', Commission de l'éthique en science et en technologie, n.d., 19, https://www.ethique.gouv.qc.ca/fr/publications/ethique-covid19/.

[24] CEST, 'CONDITIONS D'ACCEPTABILITÉ ÉTHIQUE', April 2020, https://www.ethique.gouv.qc.ca/media/1329/cest-conditions-acceptabilite-ethique_v7.pdf.

[25] 'Les enjeux éthiques de l'utilisation d'une application mobile de traçage des contacts dans le cadre de la pandémie de COVID-19 au Québec', n.d., 78.

[26] 'Cadre de réflexion sur les enjeux éthiques liés à la pandémie de COVID-19', n.d., 19.

[27] 'Les enjeux éthiques des applications anti-pandémie', *Centre de recherche en éthique* (blog), 10 April 2020, http://www.lecre.umontreal.ca/les-enjeux-ethiques-des-applications-anti-pandemie/.

[28] 'OBVIA - Applications de traçage COVID-19', Google Docs, n.d., 19, https://docs.google.com/spreadsheets/d/12283mTnvhRgVUk1QCCOcs1gZZn4TgWA837LdxVRb49k.

De multiples classifications de ces applications de traçage sont possibles. Par exemple, des chercheurs de l'OBVIA ont participé à la production d'un rapport de la *Human Technology Foundation*[29] à propos de la gouvernance des solutions technologiques dans un contexte de crise sanitaire, et qui classe ces technologies selon leur finalité : traçage des individus porteurs du virus, étude des pratiques collectives, contrôle du respect des mesures sanitaires, et contrôle de l'accès à des espaces privés.

Dans le présent document, la typologie des applications de traçage est conduite présente l'amplitude des options technologiques et stratégiques des différentes applications de traçage déployées dans le monde. Il s'agit de comprendre les technologies en expliquant leurs principes de fonctionnement, et en réalisant une évaluation descriptive et objective. En filigrane, cette analyse des caractéristiques technologiques des solutions révèle les avantages et inconvénients et les éléments importants à considérer avant un processus de conception ou un processus de sélection. Le choix d'une technologie, les considérations d'enjeux éthiques, et la détermination d'un mode de gouvernance sont tous trois entrelacés.

Les applications de traçage diffèrent les unes des autres selon de nombreux critères que nous pouvons classer en quatre grandes catégories : [1] Finalité, [2] Données, [3] Technologies et protocoles et [4] Légitimité et encadrement légal

[1] Finalité : Les applications de traçage peuvent être classées selon leurs objectifs (primaires, secondaires et tertiaires) et selon à qui elles s'adressent (population générale, personnel de santé, cas positifs avérés, personnes à risque, personnes handicapés, travailleurs sur le lieu de travail, etc.)

[2] Données : Selon les objectifs de l'application de traçage, plusieurs types d'informations sont utilisées. Ces informations peuvent être recueillies de différentes façons, à des fréquences variables et en plus ou moins grandes quantités. Certaines données recueillies sont personnelles et confidentielles. Ces applications peuvent transformer/collecter les données de façon anonymes, pseudonymes, ou agrégées. Le cycle de vie des données peut changer selon les applications, et il peut y avoir des différences sur les modalités de stockage et d'échange des données, le lieu de conservation et la durée de conservation. De plus, selon les cas, les données seront détruites (avec différents moyens et sous la responsabilité de différentes autorités) ou conservées pour être réutilisées dans le futur pour une autre finalité.

[3] Technologies et protocoles : Les applications de traçage peuvent s'appuyer sur différents moyens techniques pour réaliser la collecte, l'analyse, et l'échange des données. Il peut y avoir différents protocoles de traitement des données qui peuvent varier selon le système d'exploitation du téléphone intelligent ou la technologie utilisée (Bluetooth et GPS).

[4] Légitimité et encadrement légal : Parmi les applications de traçage, certaines sont officiellement soutenues par le gouvernement local et peuvent être imposées ou recommandées. Dans certain cas

[29] 'Optic - Élaboration et Gouvernance Des Solutions Technologiques Pour Une Sortie de Crise Sanitaire', n.d., http://opticteчhnology.org/index.php/fr/news-fr/225-elaboration-et-gouvernance-des-solutions-technologiques-pour-une-sortie-de-crise-sanitaire.

une législation spéciale est mise en place par les autorités pour encadrer le déploiement et l'utilisation de ces outils. Souvent, la gestion des données personnelles des applications de traçage s'inscrit dans un contexte légal plus large, comme par exemple le RGPD commun à l'ensemble de l'Union européenne. Enfin, ces outils peuvent avoir fait l'objet d'audit ou d'étude d'impact sur la vie privée et les données personnelles avant d'avoir reçu le soutien du gouvernement.

D'autres facteurs peuvent permettre de mieux saisir le contexte de développement et de déploiement de l'application, comme par exemple la gravité de la situation dans la région ou le pays concerné, les facteurs culturels, ou le niveau de cohésion entre la population et le gouvernement. Cependant dans cette partie du document, ces paramètres seront peu ou pas du tout explorés. Ces enjeux pourraient être considérés dans une étude sur les facteurs de réussite liés au déploiement des applications de traçage et les modes de gouvernance.

Nous allons décrire plus en détails ces quatre grandes catégories de critères qui ont été utilisés pour classer les applications de traçage.

3.1. Finalités

Une seule application de traçage peut combiner de multiples fonctionnalités en vue d'atteindre plusieurs objectifs distincts. Certains objectifs sont dits primaires et d'autres secondaires (on entend par objectif primaire un impact direct et immédiat sur l'utilisateur de l'application ; on entend par objectif secondaire tout autre objectif atteint ou tout autre bénéfice obtenu par extension de l'utilisation de l'application, que ce soit pour l'utilisateur ou une autre entité).

Les deux types de traçage, le *traçage de contact* et le *suivi de position*, n'aboutissent pas forcément aux mêmes objectifs.

Objectifs primaires

Traçage de contact : établir un historique de contacts (promiscuité, durée) entre les utilisateurs, et en cas de test se révélant positif, établir les contacts présentant un risque de contagion. Ces applications ont pour objectifs principaux de :

- Recenser les utilisateurs qui se sont exposés à un risque
- Suivre les contacts entre les personnes en cas de risque de transmission du virus
- Aviser automatiquement les personnes ayant rencontré une personne testée positive pour permettre aux personnes à risque de gérer leur isolement
- Prévenir les infections en chaîne (circonscrire les infections, limiter les épisodes de contagion)
- Donner un sentiment de sécurité et/ou de contrôle de la situation à l'utilisateur. (Fournir un outil permettant à chacun d'examiner son statut, d'enregistrer ses interactions physiques

avec d'autres personnes « au cas où » offre un sentiment rassurant de contrôle, et la capacité d'être averti et de réagir rapidement).

Suivi de position : pister la localisation d'une personne testée positive afin de s'assurer qu'elle ne met pas d'autres personnes en danger d'infection. Ces applications ont pour objectifs principaux de :

- Suivre la position et les déplacements des personnes porteuses du COVID-19
- Aviser les propriétaires immobiliers et les employeurs du fait qu'une ou des personnes testées positives ont été sur les lieux, et gérer les cas nécessitant des fermetures d'immeubles ou de lieu de travail
- Contrôler l'accès à des espaces privés
- Contrôler l'accès à des lieux sensibles (cliniques, hôpitaux, écoles)
- Contrôler les mesures strictes d'isolement en avertissant les autorités si une personne quitte sa zone de quarantaine et/ou pénètre dans un lieu qui lui est momentanément interdit ou à haut risque (lieu public fréquenté, lieu avec des personnes à risque)

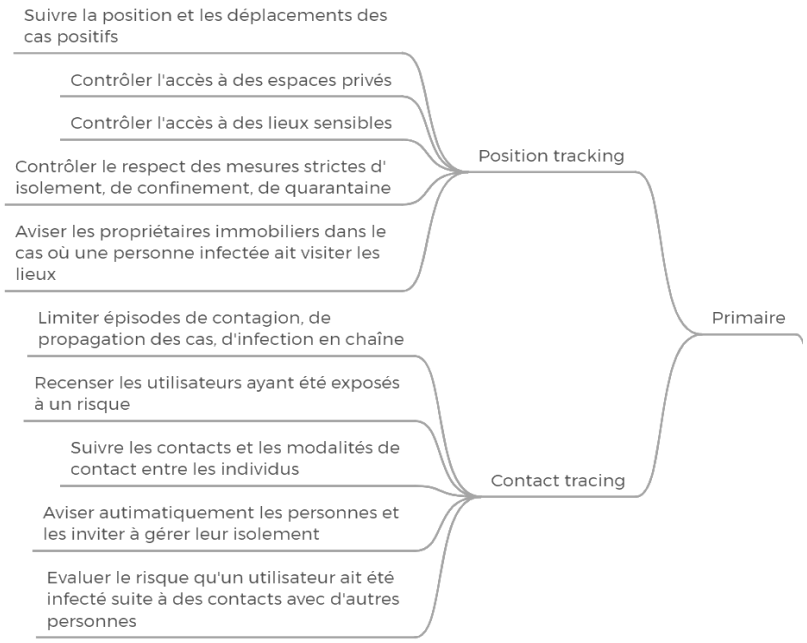

Illustration 2. Classification des objectifs primaires des applications de traçage.

Objectifs secondaires

Les objectifs secondaires peuvent être à la fois dérivés des applications de *traçage de contact* ou des applications de *suivi de position*. Ces objectifs se fondent sur la capacité d'agréger les données de tous les utilisateurs de l'application – ils sont de plus grande envergure, et ils visent le moyen et le long terme.

Épidémiologie et système de santé

- Suivre l'évolution de la pandémie : les données agrégées sont un proxy pour mesurer l'état de la situation à un instant précis, à l'instar du nombre de personnes testées ou du nombre de personnes hospitalisées. C'est un moyen pour les autorités d'être informées dans un délai proche du temps réel de la propagation du virus ;
- Suivre en temps réel de la propagation du virus qui autorise des prédictions plus précises des tendances d'évolution, et par conséquent l'anticipation des besoins et des moyens à mettre en œuvre localement (dans les cliniques ou les hôpitaux). Cette anticipation permet non seulement d'organiser les ressources, mais aussi d'émettre des messages à caractère informatifs pour la population ;
- Surveiller l'afflux des personnes dans des lieux de rassemblement ou des lieux publics, s'assurer qu'un seuil sécuritaire n'est pas dépassé, et organiser une intervention si nécessaire ;
- Mettre en lien avec le système de santé : recommandation de consultation virtuelle, orientation vers une clinique spécialisée pour un rendez-vous réel, avis de procéder à un test de dépistage ; triage ;
- Évaluer l'efficacité des mesures de politiques publiques mises en place pour diminuer la propagation du COVID-19 : suivant l'évolution du nombre de cas, les autorités pourraient alléger ou renforcer certains dispositifs ;
- En situation réelle, identifier les principaux vecteurs et facteurs de contamination pour nourrir la prise de décision quant aux mesures les plus adéquates ; améliorer la compréhension des facteurs de risques pour les individus et des probabilités de contagion suivant les profils de santé ;
- Cartographier le risque de transmission par zone, par région, voire par communauté ; permettre le suivi local des cas actifs.

Étude des comportements individuels et des pratiques à l'échelle de la société

- Mesurer l'efficacité des règles de conformité, étudier le comportement des personnes en situation de confinement (aversion au risque, tendance à respecter ou non les recommandations ou les interdictions). Ces informations peuvent souligner la nécessité de mettre en place des règles additionnelles de prévention, de contrôle, voire des mesures punitives, dans le but d'atteindre les objectifs de confinement ;

- Limiter ou réguler les déplacements et voyages non-autorisés, et par conséquent les situations à risque ;
- Améliorer la compréhension des vecteurs de transmission du virus pour faire évoluer les solutions de détection et de prévention, et par extension fournir les moyens nécessaires à la population et au système de santé ;
- Étudier les comportements individuels et collectifs de la population dans un contexte de pandémie, et donc de peur : « exode » de centre urbains vers les régions moins densément peuplées ; respect ou non du confinement, tendance à respecter les règles et les seuils d'acceptabilité des mesures ; comportements économiques (priorités des dépenses) et sociaux (activités quotidiennes, emploi, cercle social).

Parmi les objectifs secondaires figure aussi l'opportunité d'alimenter en données la recherche académique, visant par exemple à faciliter la lutte future contre d'autres pandémies futures, et à analyser – à rebours – les réponses et les dispositifs mis en place pour faire face à la COVID-19.

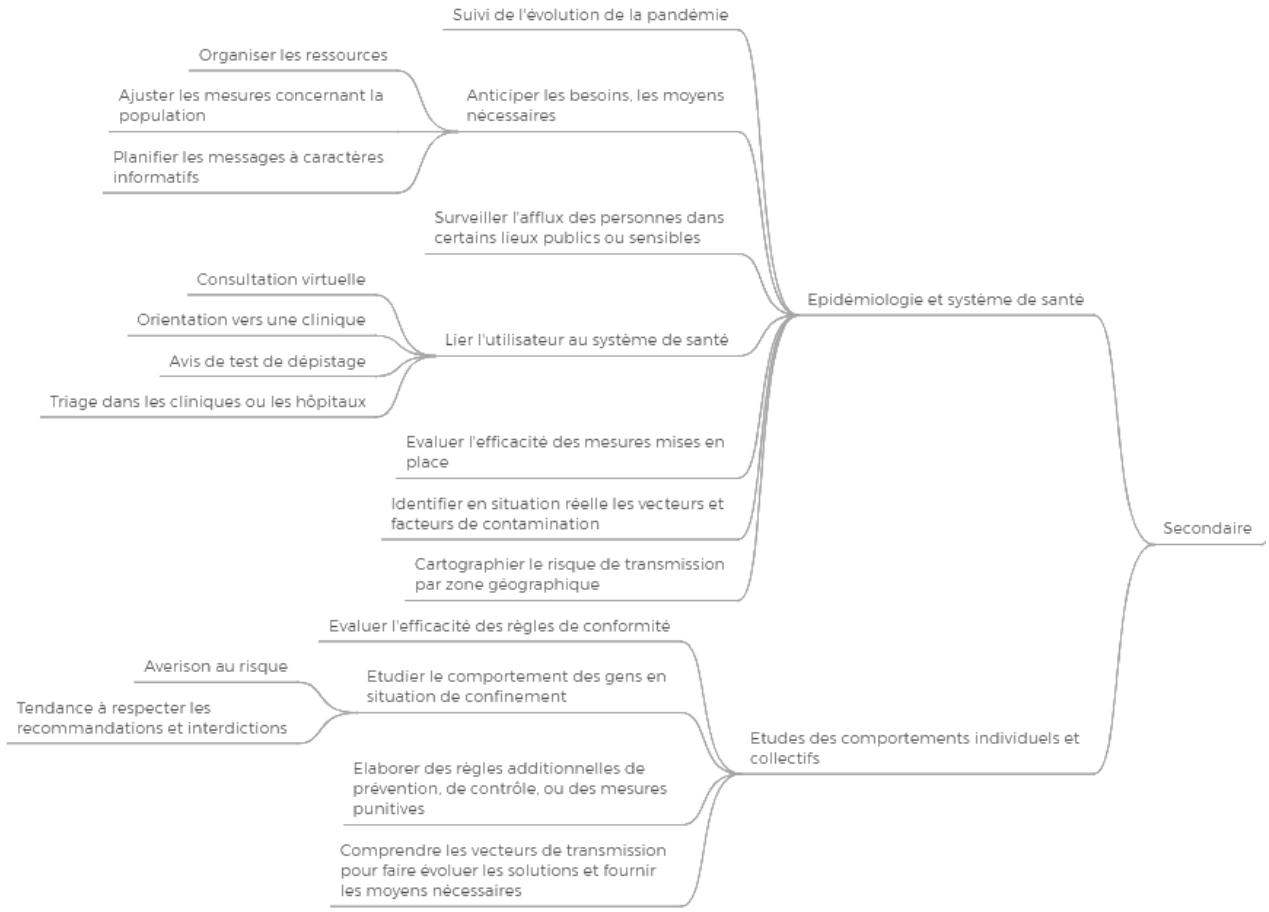

Illustration 3. Classification des objectifs secondaires des applications de traçage.

Objectifs tertiaires

Les objectifs tertiaires présentent un caractère plus global et sont atteints lorsque la crise sanitaire est contenue et réduite. Ces objectifs sont atteints par extension, et peuvent être appréciés comme les motivations qui poussent à déployer les solutions technologiques comme les applications de traçage.

- Reprise de la vie normale :
    - Reprise du travail
    - Reprise de l'activité économique
    - Reprise de la vie sociale
    - Reprise des activités de distraction
    - Reprise des activités sportives
    - Reprise des activités culturelles
- Réduire les impacts psychologiques causés directement ou indirectement par la crise sanitaire (dus à l'isolement, la quarantaine, la diminution des contacts sociaux, etc.). Ces impacts sont atténués en ramenant la population à une vie quotidienne normale et en lui donnant le contrôle d'outils qui lui permettent de gérer le risque de la maladie.
- Préserver la sécurité de toute la population, notamment dans les situations où une structure ou une organisation a un devoir de responsabilité vis-à-vis des personnes qui en dépendent. Par exemple :
    - L'employeur vis-à-vis des employés ;
    - Le système éducatif vis-à-vis des professeurs et des élèves ;
    - Les commerces vis-à-vis des clients ;
    - Les organismes de transports en commun vis-à-vis de leurs usagers ;
    - Le système de santé vis-à-vis des professionnels de santé et des patients.

Les applications de traçage ont pour but principal de mesurer la propagation du virus dans la population tant à l'échelle individuelle qu'à l'échelle collective, et par conséquent visent à limiter les risques pour la population et circonscrire les impacts sur la société.

À l'échelle individuelle, les applications de traçage permettent de prévenir l'ensemble de la chaîne des personnes connectées à un individu testé positif, et donc d'assurer une forme de prévention en contenant la propagation du virus et en recommandant aux utilisateurs les bonnes pratiques à suivre (par exemple aller se faire dépister). Aux capacités de traçage, l'ajout de la fonctionnalité d'auto-évaluation (le calcul du risque, de la probabilité d'être infecté par le virus), en général réalisée via une série de questions sur les symptômes de l'utilisateur, permet d'anticiper l'apparition de symptômes graves chez l'utilisateur et par conséquent de limiter la période où celui-ci pose un risque de contamination. Le plus tôt le risque d'être infecté est détecté, le plus vite la personne peut prendre des mesures pour limiter ses contacts physiques avec d'autres individus et aller se faire tester.

À l'échelle collective, les informations recueillies à l'aide des applications de traçage peuvent permettre d'obtenir une meilleure compréhension des facteurs favorisant la transmission du virus et l'éclosion de foyers de contamination. Ces informations sont cruciales pour aiguiller les politiques de santé publique. Le traçage des individus permet aussi de mesurer l'impact des mesures de confinement, de quarantaine, ou d'isolement. Ainsi, le traçage permet d'assurer la fonction de barrière pour les individus testés positifs en vérifiant qu'ils ne quittent pas leur domicile, ou n'accèdent pas à des lieux qui leur sont interdits. Cette utilisation revêt un côté plus liberticide et plus punitif, et doit être associée à l'adoption de mesures juridiques et légales spécifiques pour appuyer les forces de l'ordre. Ces « clôtures numériques » (*Digital fencing*) peuvent être mise en place à l'aide par exemple de bracelets électroniques ou de code QR (*QR Code*, pour *Quick Response Code*).

Par définition, les applications de traçage vont suivre l'individu en tout temps et enregistrer des paramètres sur ses déplacements, ses interactions, ses activités, son cercle social, et son état de santé. Plusieurs technologies existent pour récolter ces informations de localisation, de déplacement, ou de contact entre les personnes.

3.2. Données

3.2.1. Récolte des données de position et des données de contact

La clef de voûte du fonctionnement des applications de traçage est la capacité de recueillir des informations sur la localisation et les déplacements des utilisateurs (*position tracking*), ou la capacité d'enregistrer les contacts s'établissant entre deux utilisateurs et de consigner leur nature et leur degré (*contact tracing*). De nombreux moyens technologiques sont disponibles pour réaliser ces fonctions, en particulier la géolocalisation par GPS (*Global Positioning System*) et l'enregistrement des échanges entre deux appareils par Bluetooth (parfois BLE ou BT LE pour *Bluetooth Low Energy*). Dans un cas comme dans l'autre, ces deux technologies sont largement démocratisées puisque l'ensemble des téléphones intelligents en sont équipés.

Localisation par GPS

Sur un téléphone intelligent, le GPS utilise le principe de trilatération et capte les signaux de quatre satellites pour calculer la longitude, la latitude, et l'altitude de l'appareil récepteur. Trois signaux sont utilisés pour déterminer la position, et le quatrième sert à l'horodatage, c'est-à-dire l'information très précise sur la date est l'heure permettant de synchroniser les signaux et procéder au calcul de la position. À titre d'illustration, un problème de synchronisation d'une microseconde entre les signaux conduit à une erreur de calcul de la position de plus de 300 mètres.

La précision moyenne de la position des téléphones intelligents obtenue par GPS est de l'ordre de 4,9 mètres dans des conditions parfaites[30], et l'erreur augmente lorsque les conditions ne sont pas

[30] 'GPS.Gov: GPS Accuracy', n.d., https://www.gps.gov/systems/gps/performance/accuracy/.

idéales pour la propagation du signal (par exemple dans un centre urbain à cause des immeubles, à l'intérieur d'un bâtiment, dans une zone avec un important relief).

Bluetooth

Le Bluetooth est une norme de communication qui permet à courte distance l'échange bidirectionnel de données en utilisant les ondes radio appartenant à une bande de fréquence particulière.

Dans le cadre des applications de traçage pour lutter contre le coronavirus, lorsque la fonction Bluetooth d'un téléphone intelligent est activée l'appareil envoie de manière continue des ondes pour signaler sa présence aux autres appareils, et capte de manière continue les ondes émises par les autres appareils. Puisque les signaux émis ne peuvent être reçus par un autre appareil que sur une courte distance, capter le signal provenant d'un autre téléphone est donc un proxy interprété comme un « contact physique » ayant eu lieu entre deux individus équipés de téléphones intelligents sur lesquels l'application est installée, contact au cours duquel la contagion du virus peut être survenue.

Le signal Bluetooth est émis par défaut, et donc à destination de tous les appareils à proximité sans distinction. Il est impossible de limiter la distance d'émission ou de réception d'un signal, et la force du signal ne peut pas servir pour calculer la distance entre deux appareils qui s'échangent le signal. En effet, de même que pour la technologie GPS, les conditions d'environnement autour de l'appareil (géométrie de la pièce, téléphone dans une poche, ou façon ou de tenir l'appareil (orientation)[31], modèle de fabrication du composant[32] (*chipset*) Bluetooth) influent sur la qualité et la force du signal. Dans des conditions optimales, un signal Bluetooth peut être capté au-delà d'une distance de 30 mètres ; à l'inverse, dans de mauvaises conditions (comme de fortes interférences) un signal entre deux appareils séparés de moins de deux mètres ne sera pas relevé. Par conséquent, utiliser la technologie Bluetooth en tant que proxy pour mesurer les contacts à risque entre les utilisateurs d'une application de traçage peut conduire à un risque de sur-déclaration et à de nombreux faux-positifs : deux utilisateurs attendant longtemps le bus dans deux sens opposés, et donc séparés par la route, pourraient être enregistrés comme ayant eu un contact prolongé et donc à risque.

Pour pallier cette limite, certaines mesures peuvent être mises en place comme la nécessité pour le rapprochement de durer une période de temps minimum. L'association du signal Bluetooth à d'autres informations ou récepteurs, comme le capteur de lumière de l'appareil photographique pour évaluer si un appareil est dans une poche, ou les accélérateurs/gyroscopes qui permettent à l'appareil de connaître son orientation dans l'espace, pourrait améliorer l'évaluation de la distance entre deux individus à partir du signal Bluetooth. Cependant d'autres limitations contextuelles à ces contacts existent : techniquement deux personnes séparées par un mur ou par une vitre sont assez

[31] Umair Mujtaba Qureshi et al., 'Analysis of Bluetooth Low Energy (BLE) Based Indoor Localization System with Multiple Transmission Power Levels', in *2018 IEEE 27th International Symposium on Industrial Electronics (ISIE)*, 2018, 1302–7, https://doi.org/10.1109/ISIE.2018.8433787.

[32] 'Bluetooth LE Chipset Guide 2019 and Beyond', Argenox, n.d., https://www.argenox.com/library/bluetooth-low-energy/bluetooth-le-chipset-guide-2019/.

proches pour que les appareils signalent un « contact à risque », bien que les deux appareils soient séparés de manière physique et qu'il n'y ait aucun risque de contagion du virus.

Malgré ces réserves sur la précision du Bluetooth pour mesurer la distance entre deux individus et le risque d'un contact contagieux, c'est bien cette méthode qui est largement utilisée et mise en avant pour expliquer la nature et le fonctionnement des applications de traçage aux utilisateurs. Par exemple dans la FAQ de l'application allemande Corona-Warn-App :

> « La distance [entre deux utilisateurs] est calculée à partir de la mesure de la réduction de la force du signal Bluetooth, qui est mesurée en dB (décibels). Toutes les expositions à partir d'une clef de diagnostic positif qui ont duré moins de 10 minutes au total (qu'importe la distance minimale) ou au cours desquelles les appareils étaient à plus de 8 mètres (73 dB d'atténuation) en moyenne (qu'importe la durée totale de l'exposition) ne sont pas enregistrées et sont défaussées comme inoffensives. »[33]

Par ailleurs, la conséquence principale du manque de précision de l'évaluation de la distance entre deux appareils par la mesure de la force du signal Bluetooth est un grand nombre de faux positifs. Cet écueil a été amplement débattu, y compris dans des études d'impacts sur la vie privée, sur les données personnelles, et sur l'efficacité de ce type de solution technologique pour lutter contre le coronavirus : bien que les faux positifs aient un coût, ils sont vu comme un coût acceptable pour la société en comparaison d'une propagation accrue de la COVID-19 dans la société.[34]

Le GPS et le Bluetooth sont les deux principales technologies utilisées pour déterminer la position et les contacts entre les personnes. Bien que ces technologies soient très démocratisées (avec une présence sur tous les téléphones intelligents) et présentent l'attrait d'une relative précision, elles ne permettent pas d'obtenir une information exacte. En absence de mise en contexte de cette information, les conclusions de l'application manquent de perspective et donc de véracité, et peuvent par conséquent conduire à des faux-positifs, des erreurs, ou des amalgames. Par comparaison, les directives de distanciation sociales fixent la limite d'une distance de deux mètres comme norme acceptable, distance qui est inférieure au seuil de précision ou de détection des signaux GPS ou Bluetooth.

La nécessité de multiplier les méthodes de mesure et d'augmenter la quantité de données collectées apparaît alors comme garanties de plus de justesse et de précision et comme impératifs pour assurer de la meilleure manière les fonctions des applications de traçage sans risquer les erreurs et les faux positifs. Cependant, plus la quantité de données collectées est grande et plus les informations sur les contacts et la position des individus sont complètes et précises, plus les enjeux éthiques et juridiques sont importants. L'intensification de la quantité de données vérifiables, échangées de manière très

[33] 'Open-Source Project Corona-Warn-App – FAQ – An Encounter Has Been Reported, but the Risk Status Stays Green', n.d., https://www.coronawarn.app/en/faq/#encounter_but_green.

[34] 'Department of Health - THE COVIDSAFE APPLICATION - Privacy Impact Assessment', 24 April 2020, https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-covidsafe-application-privacy-impact-assessment.pdf.

régulière, et provenant de multiples sources pouvant être croisées est un risque d'atteinte aux données confidentielles et personnelles de l'utilisateur. Cela va à l'encontre du principe éthique de protection de la vie privée dès la conception (*privacy by design*), et peut entrer en conflit avec les législations encadrant la protection des renseignements personnels et incluant les principes de légalité, de nécessité, de finalité, et de minimisation des données.

3.2.2 Données personnelles et anonymat

Cadre juridique et définitions des données personnelles

Il existe de nombreuses définitions pour les données personnelles, chacune ayant leurs nuances. Ces définitions sont inscrites au sein de lois écrites par les autorités législatrices souveraines, par exemple :

- Au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE, *PIPEDA*) est une loi fédérale qui définit les renseignements personnels (*Personal Information*). La législation fédérale ne s'applique qu'aux relations interprovinciales ou internationales. Elle s'applique dans les provinces lorsque celles-ci n'ont pas promulgué une législation qui justifie une exemption d'application de cette loi ;
- Au Québec, les renseignements personnels des individus sont protégés par deux lois différentes, selon qu'ils sont détenus par une entreprise privée (*Loi sur la protection des renseignements personnels dans le secteur privé*) ou par un organisme public (*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*). La Commission d'accès à l'information est l'organe québécois chargé du respect de cette législation ;
- Le *Règlement général sur la protection des données personnelles* (RGPD, *GDPR en anglais*), avec ses données personnelles (*Personal Data*), est un règlement de l'Union Européenne qui s'applique de manière extraterritoriale et qui vise à renforcer les droits des citoyens européens sur la protection de leurs données personnelles en posant des obligations pour les acteurs traitants ces données. Ce règlement substitue la directive sur la protection des données personnelles (95/46/CE) ;
- En France la *Loi Informatique et Libertés du 6 janvier 1978* a été modifiée par la *Loi du 20 juin 2018 relative à la protection des données personnelles* (pour l'adapter aux dispositions du RGPD) ;
- Aux États-Unis, le *National Institute of Standards and Technology* (NIST) définit le concept d'informations d'identification personnelles (*Personally Identifiable Information, PII*). Cette définition est utilisée dans le droit au niveau fédéral (*Privacy Act of 1974*) et étatique ;
- Au Nevada, cette définition est utilisée au sein du Chapitre 603A sur la sécurité et protection des informations personnelles (*Security And Privacy Of Personal Information*) ;
- En Californie, la loi sur la protection des données personnelles des consommateurs résidant en Californie (*California Consumer Privacy Act*, CCPA) définit les données personnelles

(*Personal Data*), en encadre les usages commerciaux, et garanti certains droits aux utilisateurs ;

- En Australie, l'*Australia Privacy Act* de 1988 définit les renseignements personnels comme toute information ou opinion qui pourrait permettre d'identifier un individu.

Les informations d'identifications personnelles sont des informations qui, utilisées seules ou avec des informations additionnelles, peuvent identifier un individu. Les informations d'identification personnelles (*PII*) peuvent être des identificateurs directs (comme un numéro de passeport) ou des "quasi-identificateurs (l'âge, la nationalité, le lieu de naissance) qui peuvent permettre une identification indirecte. Les PII peuvent être des informations cruciales comme le nom complet, le numéro de sécurité sociale, des données financières, ou encore des données médicales. D'autres PII, habituellement considérées comme basiques, sont typiquement des données de segments démographiques comme le code postal, la date de naissance, ou encore le genre. De telles informations « élémentaires » permettent d'identifier une large portion de la population[35].

Au travers de la LPRPDE, le droit canadien définit un renseignement personnel :

> « Tout renseignement factuel ou subjectif, consigné ou non, concernant une personne identifiable. Il peut s'agir de tout type de renseignement, par exemple :
>
> - L'âge, le nom, un numéro d'identification, le revenu, l'origine ethnique ou le groupe sanguin;
> - Une opinion, une évaluation, un commentaire, le statut social ou une mesure disciplinaire;
> - Le dossier d'un employé, un dossier de crédit ou de prêt, un dossier médical, l'existence d'un différend entre un consommateur et un commerçant ou le projet d'une personne (par exemple, l'intention d'acquérir des biens ou des services ou de changer d'emploi). »

En comparaison du droit canadien et américain, le RGPD a une définition particulièrement plus large des données personnelles pour inclure toute information qui identifie ou rend identifiable, directement ou indirectement, un individu.

> « Données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » RGPD ; Article 4, 1.

Suivant la législation en vigueur et surtout l'interprétation des définitions, une donnée peut être ou ne pas être qualifiée de donnée personnelle. Des décisions de justice aux États-Unis ne s'accordent pas sur la classification de l'adresse IP. Certaines décisions qualifient l'adresse IP non pas d'information d'identification personnelle (PII), mais de « *Linked-PII* » :

[35] Latanya Sweeney, 'Simple Demographics Often Identify People Uniquely', . . *Pittsburgh*, n.d., 34.

> « [in] order for 'personally identifiable information' to be personally identifiable, it must identify a person. But an IP address identifies a computer. »

Plus récemment, des guides[36] publiés par la Commission fédérale du commerce des États-Unis (*Federal Trade Commission, FTC*) nuancent ces classifications des données dans l'une ou l'autre catégorie :

> « [W]e regard data as 'personally identifiable,' and thus warranting privacy protections when it can be reasonably linked to a particular person, computer, or device. In many cases, persistent identifiers such as device identifiers, MAC addresses, static IP addresses, or cookies meet this test. »

D'autres législations américaines associent la catégorisation de la donnée à la finalité et à la possibilité de l'association d'une identité à la donnée, comme par exemple en Californie :

> « personal information include[s] online identifiers such as an IP address, but only if the identifier identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household »

Au Canada, le Commissariat à la protection de la vie privée (CPVP) a conclu dans une recherche[37] publiée en mai 2013 qu'une adresse IP, combinée à d'autres renseignements de source publique, et ce, sans même avoir accès aux dossiers de l'abonné du fournisseur de services Internet (FSI), permettait de révéler l'identité du propriétaire, ainsi que ses activités de navigation sur le Web ou autres activités. En se fondant sur cette conclusion, une adresse IP peut ainsi, dans bon nombre de cas, constituer un renseignement personnel, que les dossiers de l'abonné d'un FSI liant cette adresse à une personne soient légalement accessibles ou non par l'organisation faisant la collecte de l'adresse IP.

En 2019 en France, le tribunal de grande instance de Paris a refusé d'obliger Orange (un fournisseur de services internet et de téléphonie cellulaire) à fournir des informations permettant d'identifier des contrefacteurs présumés (en litige avec une entreprise canadienne). L'ordonnance[38] du juge souligne qu'une adresse IP est bien une donnée à caractère personnelle, dont le traitement doit s'effectuer dans le respect des règles applicables au droit à la protection des données à caractère personnel.

Bouleversements numériques et réflexions pour un encadrement plus adapté

Au Québec, la Commission d'accès à l'information (CAI) partage son inquiétude quant au caractère

[36] 'Keeping Up with the Online Advertising Industry', Federal Trade Commission, 21 April 2016, https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

[37] Commissariat à la protection de la vie privée du Canada, 'Ce qu'une adresse IP peut révéler à votre sujet', 22 May 2013, https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/ip_201305/.

[38] 'TGI de Paris, Ordonnance de Référé Du 2 Août 2019', n.d., https://www.legalis.net/jurisprudences/tgi-de-paris-ordonnance-de-refere-du-2-aout-2019/.

dépassé de la protection des renseignements personnels[39]. Elle vise moins une rénovation de notions fondamentales à l'instar des travaux entrepris par le Commissariat à la vie privée du Canada. La CAI fait le constat dans son activité que les entreprises collectent des données non pertinentes dont la finalité n'a pas été consentie par le consommateur et invite le législateur à clarifier la portée de ce que le consentement autorise à recueillir.

Au niveau fédéral, le Commissariat à la protection de la vie privée émis un rapport[40] sur la sélection des priorités stratégiques liées à la vie privée. La première priorité affichée est le renforcement de la protection de la vie privée face à l'émergence de modèles économiques basés sur l'utilisation de mégadonnées. Le constat de l'archaïsme du cadre juridique est inquiétant pour les citoyens et tend à saper la confiance de la société civile qui est nécessaire à la croissance de l'environnement numérique.

Les données sensibles et la crise sanitaire

L'article 9,1 du RGPD « Traitement portant sur des catégories particulières de données à caractère personnel » précise la classe de données qualifiées de sensibles :

> « Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, **des données concernant la santé** ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. »

Cette interdiction peut être levée (article 9, 2) dans certains cas, comme dans les situations décrites à l'article 9, 2, h :

> « Le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de **diagnostics médicaux**, de la **prise en charge sanitaire ou sociale**, ou de la **gestion des systèmes et des services de soins de santé** ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou **en vertu d'un contrat conclu avec un professionnel de la santé** et soumis aux conditions et garanties visées au paragraphe 3 »;

Au Québec[41], l'urgence sanitaire déclarée le 13 mars 2020 offre des pouvoirs étendus aux autorités de santé publique :

> « [O]rdonner à toute personne, ministère ou organisme de lui communiquer ou de lui donner accès immédiatement à tout document ou à tout renseignement en sa possession, même s'il s'agit d'un renseignement personnel, d'un document ou d'un renseignement confidentiel; [...] En

[39] Commission d'accès à l'information du Québec, 'Rétablir l'équilibre - Rapport Quinquennal 2016', September 2016, https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf.

[40] Commissariat à la protection de la vie privée du, 'Priorités stratégiques liées à la vie privée du Commissariat 2015-2020 – Tracer un chemin vers une meilleure protection', 2015, 23.

[41] 'COVID-19 : Protection Des Renseignements Personnels et Sécurité de l'information | Commission d'accès à l'information Du Québec', n.d., https://www.cai.gouv.qc.ca/pandemie-de-covid-19-protection-des-renseignements-personnels-et-securite-de-linformation/.

outre, le directeur national de santé publique peut communiquer des renseignements s'il a des motifs sérieux de croire que leur divulgation peut protéger la santé de la population. »

Au-delà des définitions

Les définitions dépendent des législateurs, et l'application des lois utilisant ces définitions peut varier en fonction des acteurs judiciaire et de la situation, en particulier des circonstances d'obtention des données, de la finalité des données, et de la réelle possibilité d'identifier ou non un individu à partir de ces données.

Outre leur définition, les textes de lois qui encadrent les renseignements personnels spécifient aussi l'ensemble des mécanismes assurant la protection des individus vis-à-vis de leurs données.

Depuis 2001, il existait une décision d'adéquation entre la LPRPDE et la Commission européenne, mais avec l'arrivée du RGPD cette harmonisation a été rendue caduque, et il existe désormais d'importantes différences entre les deux législations. Par exemple, la portabilité des données et l'effacement des données (« droit à l'oubli ») sont deux droits garantis par le RGPD qui garantissent aux citoyens européens davantage de contrôle sur leurs données personnelles. Ces droits sont absents de la LPRPDE. En ce qui concerne le consentement, les règles du RGPD sont plus restrictives et un consentement explicite est obligatoire. La notion de protection de la vie privée dès la conception est inscrite dans le RGPD mais est absente de la LPRPDE, ce qui astreint les développeurs de produits et de services à intégrer les enjeux éthiques liés à la récolte, la gestion, et l'analyse des données personnelles dès le début de l'élaboration de leurs systèmes. Enfin, le RGPD confère davantage de pouvoirs aux autorités de contrôle qui disposent alors de leviers pour s'assurer de l'application du règlement (notamment grâce à des amendes).

Différentes stratégies existent pour limiter les enjeux relatifs à la confidentialité des données personnelles. En particulier, l'anonymisation est un moyen d'échapper à la réglementation sur les données personnelles puisque les informations permettant d'identifier un individu sont ôtées de l'ensemble de données.

Anonymisation

L'anonymat qualifie la qualité de ce qui est anonyme, c'est-à-dire de ce dont on ignore le nom ou l'identité. L'anonymisation est donc une technique employée pour empêcher, de manière irréversible, l'identification d'un individu à partir de données à caractère personnel.

> « 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. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. »[42]

[42] 'Règlement Général Sur La Protection Des Données (RGPD) - Règlement (UE) 2016/679 Du Parlement Européen et Du Conseil Du 27 Avril 2016 Relatif à La Protection Des Personnes Physiques à l'égard Du Traitement Des Données à

L'anonymisation offre deux protections : le respect des droits fondamentaux des personnes, et l'exploitation des données à l'origine personnelles de manière sécurisée. En France par exemple, le RGPD et la Loi Informatique et libertés s'appliquent et définissent le caractère irréversible d'identification de la personne : celui-ci doit être apprécié suivant les « moyens susceptibles d'être raisonnablement mis en œuvre ».

Dans la majorité des cas, seule la transformation des données personnelles en données statistiques mise en commun (agrégées) est une étape valide d'anonymisation. Deux grandes familles de techniques d'anonymisation existent : la randomisation et la généralisation.

- Randomisation :
    - Suppression des attributs évidents ;
    - Suppression des quasi-identifiants ;
    - Ajout de bruit dans l'échantillon de données : transformer certains attributs dans l'ensemble de données pour les rendre moins précis, tout en conservant la distribution générale.
- Généralisation : généraliser ou diluer les données en changeant les échelles ou les ordres de grandeur. Par exemple, au lieu d'avoir les âges précis, la base de données finales comprendrait des intervalles d'âge : [25 – 29] au lieu de 26.

Des techniques d'analyse plus ou moins complexes permettent d'étudier des ensembles de données pour identifier un individu dont les informations ont été anonymisées. Trois familles de techniques existent, l'individualisation, l'inférence, et la corrélation :

- L'individualisation est la capacité d'isoler un ou plusieurs attributs relatifs à un seul individu dans un ensemble de données, et par conséquent d'en déduire son identité.
- L'inférence est la capacité de déduire ou prédire la valeur d'un attribut à partir des valeurs connues d'autres attributs
- La corrélation est la capacité de lier deux jeux de données appartenant à un seul et même individu, dans deux bases de données différentes. C'est donc la capacité de faire correspondre deux ensembles d'informations dans deux jeux de données distincts, mais appartenant à un seul et même profil, soit une seule et même identité.

Pseudonymisation

Si la condition de l'irréversibilité n'est pas respectée, alors les techniques employées sont dites de pseudonymisation. La pseudonymisation vient briser le lien direct entre un ensemble de données personnelles et l'identité de l'individu, cependant elle ne garantit pas qu'en analysant les données et en établissant des corrélations, l'identité de l'individu ne puisse pas être retrouvée ultérieurement.

Caractère Personnel et à La Libre Circulation de Ces Données, et Abrogeant La Directive 95/46/CE (Règlement Général Sur La Protection Des Données)', n.d., https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679.

Les mesures de pseudonymisation sont en ce sens des moyens de sécurité pour protéger l'identité des individus, et non pour garantir leur anonymat.

> « 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. » RGPD, Article 4, 5.

En pratique, il existe plusieurs techniques de pseudonymisation :

- Le code de correspondance : il s'agit de venir supprimer de la base de données principale un ou plusieurs attributs sensibles qui permettraient l'identification de l'individu, et d'affecter un code d'identification (nombre, numéro de série, code) à chaque entrée de cette base de données. Séparément sont conservés dans un document à part chaque code et les attributs sensibles qui y sont affectés. Seule une entité ayant l'autorité d'accéder à ce document de correspondance a la capacité de prendre connaissance de l'ensemble des informations, incluant les données sensibles qui permettent d'identifier les individus.
- Le chiffrement des données avec clef(s) de correspondance. Le chiffrement, ou encore le cryptage des données, consiste à rendre les données illisibles à moins de posséder une clef spécifique qui va autoriser l'accès et la consultation des informations. La donnée « claire » est lisible par le créateur de la base de données. Par sécurité, la donnée claire est transformée, ou chiffrée, en un cryptogramme. Ce cryptogramme peut ensuite être déchiffré en donnée claire, de nouveau lisible, à condition de détenir la clef de cryptographie. Le chiffrement et le déchiffrement des données peuvent être réalisés par une clef unique (on parle de clef symétrique et de chiffrement à clef secrète), ou par deux clefs différentes (on parle de clefs asymétriques et de chiffrement à clef publique).
- La tokenisation
- La fonction de hachage, La fonction de hachage avec salage, la fonction de hachage par clef, la fonction de hachage par clef enregistrée, la fonction de hachage par clef avec suppression de la clef (chiffrement déterministe)

L'anonymat dans le contexte de la COVID-19 et des applications de traçage

Évidemment, la quantité des données collectées et le caractère confidentiel des données personnelles sont une question centrale dans la conception des applications de traçage. Le fruit des efforts de recherche de contacts ou de localisation des cas positifs peuvent être diminués s'ils ne débouchent pas sur des actions concrètes pour limiter les chaînes de contagion. Ainsi, l'identification des utilisateurs des applications de traçage est une étape délicate dont la nécessité et la mise en œuvre sont largement débattues. À travers le monde, trois approches distinctes sont employées pour régler cette question : (1) l'absence d'identification par défaut, (2) l'identification par défaut, ou (3) la connexion complète de l'identité de l'utilisateur à son application.

- L'absence d'identification par défaut : il n'y a aucun besoin de s'identifier ou de suivre une quelconque étape de vérification pour installer et utiliser l'application. En revanche, pour se signaler comme testé positif au coronavirus, une étape de confirmation (par exemple l'envoi d'un *One-Time Code* (OTC) de la part d'un laboratoire est nécessaire. Toute lien d'identification se fera avec le consentement de l'utilisateur. Les autorités peuvent par exemple proposer d'entrer en contact avec l'utilisateur en lui demandant son numéro de téléphone si un contact à risque est détecté. Cette démarche a pour but de l'orienter vers les ressources ou structures adaptés pour procéder à un test ou lui fournir les conseils adéquats pour se confiner.
- L'identification par défaut : à l'installation de l'application, une étape de vérification est nécessaire. Cette étape de vérification est dans la plupart des cas réalisés en requérant un numéro de téléphone valide. Même pour ces applications de traçage nécessitant ce type d'identification par défaut, les autorités de santé publique ne peuvent pas avoir directement accès à ce numéro de téléphone. Dans le cas où l'utilisateur est à risque à la suite d'un contact, la notification lui demandera son consentement avant de le mettre en contact avec les autorités.
- La connexion complète de l'identité de l'utilisateur : certains pays ont opté pour une solution de liaison complète entre l'individu et l'application de traçage, et ces derniers doivent fournir une vaste quantité de renseignement allant du nom complet, adresse, numéro de téléphone, numéro d'identification national (carte d'identité, passeport, numéro de sécurité social, numéro de permis de travail, photographie).

L'amplitude de ces approches reflète à la fois un souci d'efficacité du processus d'identification des cas potentiels et de chaînes de propagation du coronavirus, et un souci de confidentialité et du respect de la vie privée.

En Australie, l'installation de l'application COVIDSafe est volontaire, mais il faut fournir son nom avant de pouvoir l'utiliser.

> "[W]e are satisfied that it is reasonable for [the Ministry of] Health to collect a name from Users, as the purpose of the App is to facilitate more efficient contact tracing, and Public Health Officials will require some form of identifier to ensure they are speaking with the right person when making telephone calls to Contact Users of a Positive User" [43]

En Autriche, l'installation de l'application Stopp Corona se fait sans aucune vérification. Cependant, une étape de vérification intervient si l'utilisateur souhaite se déclarer positif à la suite d'un test. De plus, si un contact à risque est enregistré, alors le consentement de l'utilisateur est demandé avant de le mettre en relation avec les autorités de santé publique.

> "The implementation of the app without requiring the disclosure of directly personal data for the use of the basic functionalities is very welcome from the point of view of data minimisation

[43] 'Department of Health - THE COVIDSAFE APPLICATION - Privacy Impact Assessment'.

(Article 5(1)(c) GDPR) and in this respect also takes into account the requirements of Privacy by Design pursuant to Article 25 GDPR." [44]

Le concept de protection des données dès la conception (*privacy by design*) a été endossé en 2010 par des régulateurs du monde entier à l'assemblée annuelle de la *International Data Protection and Privacy Commissioners*, puis reconnu en 2012 par la FTC comme un principe clef pour la protection de la vie privée en ligne[45]. Bonne pratique fondamentale, la protection des données dès la conception n'est cependant consacrée qu'en droit européen :

> « [Mise-en-œuvre], tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. » RGPD, article 25, 1.

Cependant, la protection des données dès la conception est davantage un principe éthique qu'une contrainte, et la certification dont elle pourrait être l'objet est « volontaire et accessible via un processus transparent » (RGPD, article 42, 3).

Dans le contexte de la pandémie et des applications de traçage conçues pour protéger les individus en limitant la propagation du virus, la question de la protection des données personnelles est cruciale. La multiplication (différentes sources de données, fréquence de recueil) et la sensibilité (positionnement, données médicales) des données qui pourraient être collectées proposent des modèles dont les estimations seraient plus précises, offrant par conséquent des solutions plus efficaces. A cette inclinaison s'oppose un cadre juridique qui définit les données personnelles et en modère la collecte, la gestion, et l'usage, dans le but de protéger le public. En période de crise sanitaire, les autorités gouvernantes peuvent invoquer la protection de la santé de la population pour assouplir certaines règles concernant les données personnelles. Dans cette situation, les considérations éthiques telles que la protection des données dès la conception ou la minimisation des données sont des clefs pour orienter le développement des solutions technologique à la crise sanitaire, et trouver un équilibre entre la protection de la santé et la protection des renseignements personnels. La prise en considération de ces notions dans la conception des applications et l'inclusion du public dans des discussions et des consultations sur ces sujets sont aussi un moyen de sensibiliser celui-ci aux enjeux des applications de traçage qui le concernent, ce qui est un facteur d'acceptabilité et donc de réussite de ces solutions.

[44] Ulrich Bayer et al., 'Technical and Legal Review of the Stopp Corona App by the Austrian Red Cross', n.d., 47.

[45] 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers', Federal Trade Commission, 1 March 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

3.3. Protocoles d'échanges de données des applications de traçage

Protocoles

Un protocole est une norme, un ensemble de règles qui régit le fonctionnement des applications de traçage, et plus particulièrement les modes de communication entre deux appareils. Ces deux appareils peuvent être deux téléphones intelligents appartenant à deux utilisateurs, ou bien un téléphone intelligent et un serveur où sont stockées des données. Le protocole est donc le plan à suivre pour l'enchaînement des messages qui sont échangés, et les étapes à suivre ou les actions à réaliser pour donner suite à l'envoi et à la réception de ces messages, appelés unités de données de protocole (*Protocol Data Unit*, PDU).

Par exemple, le protocole HTTP défini la démarche à suivre lorsqu'un navigateur internet installé sur un ordinateur dialogue avec un serveur pour afficher les pages d'un site internet. Pour les applications de traçage, les protocoles sont la nomenclature à suivre pour échanger/transférer des données entre des utilisateurs, ou entre un utilisateur et un serveur central.

Les protocoles sont établis par des autorités de nature différentes (privé-compagnie, académie, autorité gouvernementale, licence partagée et ouverte). Par exemple, un protocole propriétaire est un protocole de communication dont les spécifications ne sont pas publiques, à la manière d'un logiciel propriétaire. Par nature, les protocoles sont un ensemble de normes et de standards assurant un développement et un fonctionnement harmonieux des technologies de communication. Dans le cas d'un protocole propriétaire, ces normes peuvent cependant agir comme un verrouillage technologique en devenant une référence, démocratisée et largement utilisée à travers le monde, mais toujours dépendant d'une seule entité privée qui peut le modifier à sa guise. Par définition, le recours à un protocole propriétaire va à l'encontre de la notion d'interopérabilité.

Les applications sont un plus grand ensemble, comme un logiciel, dont l'essence est de réaliser une ou plusieurs tâches précises. Les applications sont installées sur des systèmes d'opération (iOS, Android) dont elles se servent comme support pour fonctionner, et suivent des protocoles pour échanger des données.

API

Les interface de programmation d'application (*Application Programming Interface*, API) permettent à une application d'interagir avec un autre système.

Si les protocoles sont les règles élémentaires à suivre pour les échanges de données, les API sont l'interface conçu pour réaliser ces échanges de données et faciliter le dialogue entre deux systèmes différents. Les API sont une interface destinée à l'intention des développeurs d'applications et offrent un langage commun qui permet à un logiciel de communiquer et d'offrir des services à d'autres logiciels.

Google-Apple : API et protocole

Google et Apple ont joint leurs efforts pour proposer un protocole d'échange des données, ainsi qu'une API permettant de développer une application sur la base de ce protocole. Le protocole Google-Apple a été développé sous le nom de *Privacy-Preserving Contact Tracing Project*[46], et est aujourd'hui baptisé *Exposure Notification Framework*[47].

Protocoles centralisés, protocoles décentralisés

Le conception ou l'utilisation de différents protocoles pour guider le développement des applications de traçage illustres différentes approches pour solutionner la crise sanitaire. En particulier, le caractère centralisé ou décentralisé de la solution technologique apparaît comme le facteur déterminant du choix pour l'un ou l'autre type de protocole. En réalité, il n'existe pas de césure nette entre les solutions centralisées et les solutions décentralisées puisque les protocoles sont davantage hybrides : certaines étapes du protocole seront réalisées localement (sur le téléphone intelligent de l'individu) et donc de manière décentralisée, tandis que d'autres étapes seront réalisées sur un serveur après la mise en commun des données et donc de manière centralisée. Alors, la classification des protocoles d'échanges de données utilisés dans les applications de traçage tient moins à la dichotomie centralisé/décentralisé qu'à un compromis entre les avantages et les inconvénients du fonctionnement, de l'efficacité, de la structure, ou de la sécurité de la solution dans son ensemble. On parlera éventuellement de protocole majoritairement centralisé, ou majoritairement décentralisé. Le choix de réaliser une étape manière centralisée ou décentralisée tient aux considérations légales, éthiques, aux droits et aux devoirs relatifs aux données (protection, sécurité, confidentialité, anonymat, responsabilité), et enfin aux objectifs d'efficacité de la solution dans son ensemble.

Les protocoles majoritairement centralisés ont pour vocation de regrouper la responsabilité de la réalisation des fonctions essentielles sous l'égide d'une entité, sur le support d'un serveur. Le but est l'uniformité et la cohérence de la solution. Cette conception impose que l'entité ait la capacité et l'obligation d'assurer cette responsabilité, et concerne donc des organisations centrales comme un état ou un regroupement d'états (ou parfois une compagnie privée). Le serveur central doit gérer toutes les authentifications et les autorisations des utilisateurs, l'ensemble du cycle de vie de la donnée (envoi, réception, stockage, sécurité, certification, agrégation, anonymisation, destruction), la maintenance et l'évolution de l'algorithme qui va évaluer la situation de l'utilisateur et son risque d'être infecté, ou encore les requêtes d'accès aux informations (par les autorités publiques, sanitaires, académiques). La mise en commun de toutes les données, même anonymisées, offre la capacité d'analyse et de recoupement la plus poussée, d'autant qu'il est possible d'ajuster la

[46] 'Privacy-Preserving Contact Tracing - Apple and Google', Apple, n.d., https://www.apple.com/covid19/contacttracing.

[47] 'Exposure Notifications: Helping Fight COVID-19 - Google', Exposure Notifications: Helping fight COVID-19 - Google, n.d., https://www.google.com/intl/en_us/covid19/exposurenotifications/.

fréquence de téléversement des données et la nature des informations de contact et de localisation partagées (type de lieux ciblés, durée ou proximité des contacts).

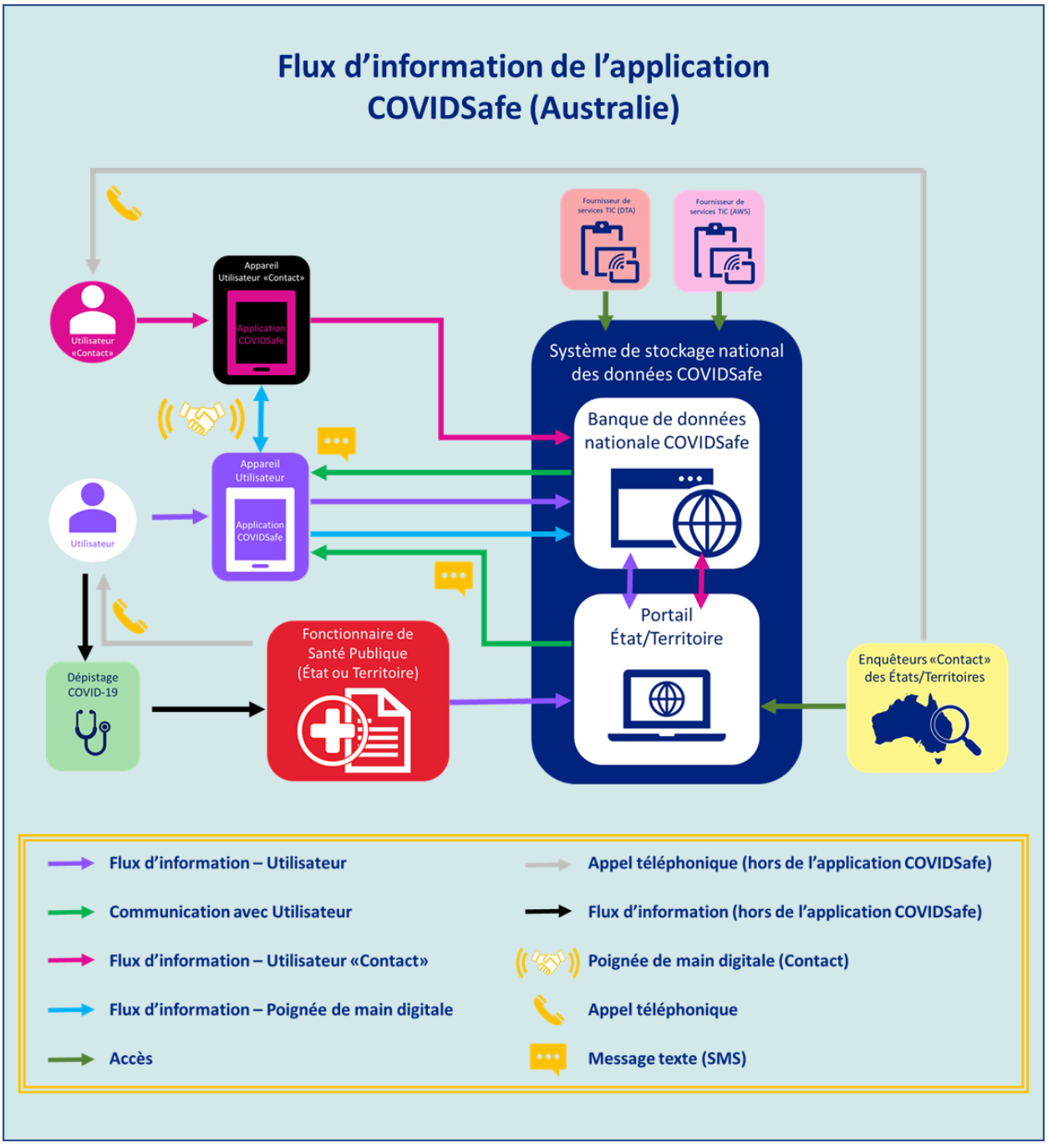

Illustration 4. Graphique des flux d'information de l'application de traçage COVIDSafe (Australie), utilisant le protocole BlueTrace (OpenTrace) et une architecture centralisée[48].

[48] 'Department of Health - THE COVIDSAFE APPLICATION - Privacy Impact Assessment'.

Cette capacité d'agir de manière cohérente et uniforme a pour conditions une confiance totale et une grande responsabilité. En effet, l'architecture centralisée comporte le risque inhérent d'être un point unique de faiblesse ou d'attaque. S'il existe une fuite ou une faille, si une erreur est commise dans le traitement des données ou le calcul du risque, c'est l'ensemble de la structure et donc des utilisateurs qui est touché. Il existe des risques de récupérer ou de manipuler l'ensemble des données, voire de mettre la main sur les identités des utilisateurs. Par exemple, au mois de mai 2020, une importante vulnérabilité dans l'application qatarie centralisée Ehteraz a exposé les informations personnelles de plus d'un million d'utilisateurs, incluant le nom, le numéro d'identification national, l'état de santé, et des informations sur le lieu de confinement[49]. Dans certains cas, si le gouvernement a confié la réalisation de l'application de traçage à une entité privée, elle lui confie par conséquent d'importantes responsabilités ; c'est le cas au Koweït, où l'entreprise Zain est chargée de la mise en œuvre de l'application de traçage Shlonik :

"Zain will take all necessary measures to ensure the appropriate level of protection and privacy of the data, including the following matters: Ensure the continued confidentiality of the application and the stored data. Restore availability and access to personal data in a timely manner in the event of a force majeure. Test and evaluate the effectiveness of security and technical measures." [50]

Les protocoles majoritairement **décentralisés** ont pour vocation la répartition des rôles et donc de la responsabilité. Le but est de créer une chaîne de responsabilité impliquant plusieurs acteurs légitimes, tenus entre eux par des mécanismes d'autorisation, de vérification, et de certification. En cas de déficience ou d'attaque sur le système, ces mécanismes (qui peuvent eux être gérés de manière centralisée) évitent de compromettre l'ensemble du système et donc l'ensemble des données et des utilisateurs. Ainsi, le gouvernement n'a pas accès aux historiques de contacts ou de déplacements qui sont enregistrés sur les appareils des utilisateurs. Généralement, les téléphones intelligents vont communiquer une ou plusieurs fois par jour avec un serveur central avec des clefs encryptées que le serveur central ne peut pas interpréter. Ces clefs sont éphémères et peuvent être générées une fois par jour ou plusieurs fois par erreur, dépendamment de la technologie employée. La comparaison avec les clefs des autres appareils reçues se fait localement, et le plus souvent le serveur central n'envoie que les clefs éphémères des appareils qui ont été signalés comme positifs.

Cette approche décentralisée est plus complexe, mais garantit un niveau supplémentaire de protection des renseignements personnels.

Alors que les premières applications de traçage commençaient leur déploiement à travers le monde en avril et mai 2020, de nombreux débat public ont éclos sur le sujet des concepts de centralisation

[49] 'Major Security Flaw Uncovered in Qatar's Contact Tracing App', n.d., https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/.

[50] 'Communication & Information Technology Regulatory Authority Security Policy for Running Electronic Applications According to The Corona Virus Emergency Services Plan (Koweit)', n.d., https://citra.gov.kw/sites/en/Pages/applications.aspx.

et de décentralisation. Outre les notions de sécurité et d'efficacité, la notion de confiance du publique a eu un poids important dans le développement des solutions décentralisées :

"A loss of confidence among the public would have endangered all the efforts of identifying and breaking infection chains early using digital support. For this reason, the Federal Government took action and adapted a decentralized approach as the project philosophy" [51]

Propriété intellectuelle

La plupart des protocoles d'échange de données utilisés dans les applications de traçage sont des protocoles open-source, c'est-à-dire dont le code est mis à la disposition de tous. La réutilisation et l'adaptation de ces protocoles pour créer des applications se fait sous la forme des licences d'utilisation, par exemple :

- La licence publique générale GNU, (GPL), qui fixe les conditions légales de distribution d'un logiciel libre du projet GNU (système d'exploitation libre)
- La licence Apache est une licence de logiciel libre et open source qui autorise la modification et la distribution du code sous toute forme (libre ou propriétaire, gratuit ou commercial) et oblige le maintien du copyright lors de toute modification (et également du texte de la licence elle-même).

Protocoles utilisés dans les applications de traçage

Decentralized Privacy-Preserving Proximity Tracing (DP-3T, voire dp3t)

Le DP-3T est un protocole développé par un regroupement de 12 universités. Il repose sur l'utilisation de la technologie Bluetooth pour enregistrer les « contacts » établis entre les utilisateurs. Lorsqu'une personne est testée positive, la conservation de l'historique des contacts permet de prévenir les utilisateurs qui encourent le risque d'avoir été contaminé. Le DP-3T a pour clef de voûte la décentralisation et l'anonymat : le protocole a été développé dans le but de conserver localement les données personnelles anonymisées grâce au chiffrement des données : l'historique des contacts d'un utilisateur est exclusivement conservé sur son appareil sans aucune référence à l'identité de l'un ou l'autre des utilisateurs.

Le développement du DP-3T a été initié en réponse aux enjeux d'anonymat et détournement possible d'un outil de traçage. La conception du protocole avait pour critère d'éviter l'enregistrement de l'identité des individus (ainsi que d'éviter toute implication avec les réseaux sociaux), se prémunir de tout risque de piratage d'un serveur central (perte ou destruction, vol, ou manipulation des données), empêcher le détournement de l'outil pour créer une base de données centrale permettant de faire de la surveillance de masse.

[51] 'Open-Source Project Corona-Warn-App – FAQ – What Were the Reasons for Favoring the Decentralized Approach to Exposure Tracing?', n.d., https://www.coronawarn.app/en/faq/#reasoning_decentralized.

Apple Inc. & Google : Exposure Notification Framework[52]

Le Système de Notification d'Exposition (*Exposure Notification System*, ou *Exposure Notification Framework*, anciennement *Privacy-Preserving Contact Tracing Project*) est un protocole développé conjointement par les compagnies Apple Inc. et Google. Ce protocole a pour objectif de minimaliser les contraintes et risques vis-à-vis de la confidentialité des informations personnelles et de la vie privée des utilisateurs. Ce protocole a par ailleurs été développé conjointement par les deux firmes pour répondre aux problématiques de dialogue entre les applications installées sur des appareils dont les systèmes d'opération (*Operating System*, *OS*) diffèrent, résolvant ainsi les problèmes de compatibilité et d'intégration entre les systèmes d'opération iOS (pour les téléphones intelligents d'Apple Inc.) et Android (pour une large majorité des autres téléphones intelligents). Le développement de ces protocoles par les développeurs des OS permet aussi un meilleur fonctionnement en tâche de fond sur les appareils, chose qui n'était pas possible, ou pas toujours possible, pour les autres applications de traçage (reposant sur d'autres protocoles) auxquelles les droits et permissions d'agir sur le fonctionnement de l'appareil n'est pas accordé. Cette fonctionnalité, ou plutôt l'absence de fonctionnalité de marche en veille, requiert alors d'avoir son téléphone constamment déverrouillé et l'application de traçage lancée et ouverte pour fonctionner correctement.

Apple Inc. et Google ont publié des lignes directrices que les développeurs d'application de traçage doivent suivre afin d'avoir l'autorisation de publier leur solution sur les plateformes servant de librairie ou de magasin d'application (respectivement l'App Store et le Google Play Store). Si le protocole *Exposure Notification Framework* n'est pas celui utilisé pour l'application, alors une évaluation du fonctionnement de l'application et de ses impacts sur la confidentialité des informations personnelles est réalisée.

Le protocole suit un processus décentralisé semblable au DP-3T et au TCN, et est en pratique une variante du DP-3T fonctionnant comme expliqué précédemment directement au niveau de l'OS[53]. Sans être absous de tout défaut, plusieurs organisations telles que l'Union américaine pour les libertés civiles (*American Civil Liberties Union*, *ACLU*) ont émis des avis positifs à propos des fonctionnalités du protocole développé par Apple Inc. et Google et des risques pour la vie privée et les informations personnelles des utilisateurs.

> « To their credit, Apple and Google have announced an approach that appears to mitigate the worst privacy and centralization risks, but there is still room for improvement. »[54]

---

[52] 'ExposureNotification | Apple Developer Documentation', n.d., https://developer.apple.com/documentation/exposurenotification.

[53] Belgium Corona App Task Force, 'Coronalert: A Distributed Privacy-Friendly Contact Tracing App for Belgium', 5 August 2020, https://www.esat.kuleuven.be/cosic/sites/corona-app/wp-content/uploads/sites/8/2020/08/coronalert_belgium_description_v1_2.pdf.

[54] 'ACLU Comment on Apple/Google COVID-19 Contact Tracing Effort', American Civil Liberties Union, n.d., https://www.aclu.org/press-releases/aclu-comment-applegoogle-covid-19-contact-tracing-effort.

Pour des raisons d'efficacité (fonctionnement de l'application reposant sur ce protocole en tâche de fond de l'OS avec des privilèges par rapport aux autres applications), d'intégration et d'interopérabilité (entre les différents appareils sur différents OS), et du dessin affirmé de décentralisation dans une optique de confidentialité des données personnelles des utilisateurs, de très nombreux gouvernements ou autorités de santé publique ont développé et publié une application de traçage reposant sur l'*Exposure Notification Network*, bénéficiant du support des firmes dans la conception de la solution technologique. Il existe aujourd'hui plus d'une vingtaine d'applications développées à partir du protocole d'Apple Inc. et Google.

Tableau 2. Gouvernements ayant développé et déployé une application utilisant le protocole *Exposure Notification Network* — Déploiement réalisé ou en cours.

Gouvernement	Nom de l'application	Gouvernement	Nom de l'application
Afrique du Sud	COVID Alert SA	Japon	COCOA
Alabama (État s-Unis)	GuideSafe	Lettonie	Apturi Covid
Alberta (Canada)	COVID Alert / Alerte COVID	Manitoba (Canada)	COVID Alert / Alerte COVID
Allemagne	Corona-Warn-Aoo	New Jersey (États-Unis)	COVID Alert NJ
Angleterre (Royaume-Uni)	NHS COVID-19	New-York (États-Unis)	COVID Alert NY
Arizona (États-Unis)	Covid Watch	Nouveau-Brunswick (Can.)	COVID Alert / Alerte COVID
Autriche	Stop Corona App	Nouvelle-Écosse (Canada)	COVID Alert / Alerte COVID
Belgique	Coronalert	Ontario (Canada)	COVID Alert / Alerte COVID
Brésil	Coronavirus-SUS	Pays de Galles (R-U)	NHS COVID-19
Caroline du Nord (É-U)	SlowCOVIDNC	Pays-Bas	CoronaMelder
Dakota du Nord (États-Unis)	Care19 Alert	Pennsylvanie (États-Unis)	COVID Alert PA
Danemark	Smittestop	Pologne	ProteGO Safe
Delaware (États-Unis)	COVID Alert DE	Portugal	STAYAWAY COVID
Écosse (Royaume-Uni)	Protect Scotland	Québec (Canada)	COVID Alert / Alerte COVID
Espagne	RadarCOVID	République Tchèque	Rouska
Estonie	Hoia	Saskatchewan (Canada)	COVID Alert / Alerte COVID
Finlande	Koronavilkku	Suisse	SwissCovid
Gibraltar	BEAT Covid Gibraltar	Terre-Neuve-et-Labrador (Ca.)	COVID Alert / Alerte COVID
Île-du-Prince-Édouard (Can.)	COVID Alert / Alerte COVID	Uruguay	Coronavirus UV
Irlande COVID	Tracker Ireland	Virginie (États-Unis)	COVIDWise
Irlande du Nord (R-U)	StopCOVID NI	Wyoming (États-Unis)	Care19 Alert
Italie	Immuni		

ROBust and privacy-presERving proximity Tracing protocol (ROBERT)[55] [56]

Le protocole ROBERT (traduction du sigle : Traçage de la proximité robuste et préservant la vie privée) est une proposition qui fait suite à une initiative paneuropéenne de suivi des contacts de proximité préservant la vie privée (PEPP-PT). Il a été développé spécifiquement pour l'application StopCovid France, avec pour but principal de garantir le respect des normes européennes en matière

[55] INRIA, 'Protocole ROBERT - Un Protocole de Suivi Des Contacts Rapprochés, Rigoureux et Respectueux de La Vie Privée.', n.d., https://www.inria.fr/sites/default/files/2020-04/Pr%C3%A9sentation%20du%20protocole%20Robert.pdf.

[56] INRIA, 'Du Protocole à l'application StopCovid' (INRIA, n.d.), https://www.inria.fr/sites/default/files/2020-05/From%20protocole%20to%20application.pdf.

de protection des données, de vie privée et de sécurité. Il a été développé en commun par deux entités : l'équipe PRIVATICS de l'Inria (France) et la branche AISEC (*Applied and Integrated Security*) de l'institut Fraunhofer (Allemagne).

À la suite d'un test de dépistage positif, l'appareil d'un utilisateur de l'application transmet à des serveurs centraux les pseudonymes éphémères des identifiants des autres téléphones avec lesquels il a été en « contact ». Chaque appareil muni de de l'application consulte périodiquement cette base de données centralisée et vérifie si l'un de ses pseudonymes éphémères y figure, signe que son utilisateur encoure un risque d'exposition au COVID-19.

ROBERT est un protocole qualifié de centralisé puisque si l'étape de collection et de cryptage des données de contact est décentralisée (effectuée localement sur l'appareil de l'utilisateur), les clefs de de codage, l'ensemble des données de contact, et l'étape d'évaluation du risque d'infection sont sauvegardées ou s'effectuent de manière centralisée.

Il est à noter que quelques temps après le développement de ROBERT et avant l'implantation de l'application StopCovid France qui utilise ce protocole, des responsables de l'Inria ont publié une autre solution hybride (au sens des approches centralisée et décentralisée), le protocole DÉSIRÉ[57]. La principale différence est la manière dont deux appareils interagissent ensemble : au lieu d'échanger les identifiants éphémères de chaque appareil, des jetons privés de rencontre (*Private Encounter Tokens*, *PET*) sont créés spontanément, conjointement, et de manière confidentielle par les applications des deux utilisateurs qui entrent en « contact ». Cette origine locale est une composante de la décentralisation de l'ensemble du processus[58] :

> [L]'utilisation de deux listes de jetons PET par application garantissent un niveau élevé de confidentialité au protocole DESIRE. De plus, avec le chiffrement systématique de chaque inscription dans la base de données du serveur, les clés de déchiffrement étant conservées par les clients, DESIRE se caractérise également par une forte résilience face aux risques de fuites de données du serveur[59].

Présentement, ROBERT est encore le protocole sur lequel repose le fonctionnement de l'application StopCovid France.

Tableaux comparatifs des protocoles de traçage

La centralisation et la décentralisation des données sont souvent présentées comme une dichotomie franche, mais il convient de décomposer les phases de fonctionnement des protocoles de traçage, la succession des étapes d'échanges des données entre les différents acteurs et les différentes structures.

---

[57] Vincent Roca et al., 'DESIRE: une Troisième Voie pour un Système Européen de Notification d'Exposition', n.d., 6.

[58] L'Usine Nouvelle, 'En quoi consiste le protocole Désiré, la troisième voie de l'Inria pour l'application StopCovid ?', 14 May 2020, https://www.usinenouvelle.com/editorial/en-quoi-consiste-le-protocole-desire-la-troisieme-voie-de-l-inria-pour-l-application-stopcovid.N964166.

[59] Roca et al., 'DESIRE: une Troisième Voie pour un Système Européen de Notification d'Exposition'.

Tableau 3. Étapes du processus de collecte et d'analyse des données selon 6 protocoles.

Étapes/ Protocoles	Système de Notification d'Exposition	BlueTrace / Open Trace	Coalition TCN	COVI (MILA)	DP-3T	ROBERT
Collecte des données	Décentralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Chiffrement des données	Décentralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Génération des clefs de chiffrement	Décentralisé	Centralisé	Décentralisé	Décentralisé	Décentralisé	Centralisé
Stockage des données	Décentralisé	Décentralisé	Centralisé	Centralisé	Centralisé	Centralisé
Évaluation du risque	Décentralisé	Centralisé	Décentralisé	Décentralisé	Décentralisé	Centralisé
Échange des données lors de l'évaluation du risque	N/A	Envoi de ses propres clefs de contacts	Réception des clés des contacts des utilisateurs infectés	Réception des clés des contacts des utilisateurs infectés	Réception des clés des contacts des utilisateurs infectés	Envoi de ses propres clefs de contacts
Échange des données si l'utilisateur est testé positif	Envoi de ses propres clefs de contacts	Envoi des clefs des autres contacts	Envoi des clefs des autres contacts	Envoi de ses propres clefs de contacts et des informations de localisation brouillées	Envoi des clefs des autres contacts	Envoi des clefs des autres contacts

Tableau 4. Autres critères d'évaluation des protocoles.

Critères/ Protocoles	Système de Notification d'Exposition	BlueTrace / Open Trace	Coalition TCN	COVI (MILA)	DP-3T	ROBERT
Collecte des données	Bluetooth	Bluetooth	Bluetooth, GPS	Bluetooth, GPS	Bluetooth	Bluetooth
Collecte des données des utilisateurs privés	Non	Non	Non	Non	Non	Non
Collecte de données additionnelles	Non	N/A	Localisation	Localisation	N/A	Localisation possible
Évaluation prédictive	Non	Non	Non	Oui	Non	Non
Autres utilisations envisageables	Non	Non	Non	Recherche académique	Non	Incertain
Intervention d'un personnel de santé ou agent gouvernemental	Oui	Oui	Oui	Oui	Oui	Oui
Complexité de la structure du serveur	À déterminer	À déterminer	À déterminer	À déterminer	À déterminer	À déterminer
Sécurité de la structure du serveur	À déterminer	À déterminer	À déterminer	À déterminer	À déterminer	À déterminer
Ouverture du code	Oui	Oui	Oui	Oui	Oui	Non
Origine et/ou gouvernance	Apple Inc. et Google	Gouvernement Singapour, gouvernement local	O.B.N.L.	Institut des algorithmes d'apprentissage de Montréal (MILA), O.B.N.L.	O.B.N.L.	Inria et institut Fraunhofer, Gouvernement Français

Tableau 5. Grille de comparaison des protocoles utilisés pour les applications de traçage, issue de l'Élaboration et gouvernance des solutions technologiques pour une sortie de crise sanitaire[60] (publication le 27 avril 2020)

Comparaison uniquement fondée sur des aspects de la (dé)centralisation et des caractéristiques de haut niveau pour lesquels il existe des différences importantes.

Catégories	ROBERT	DP-3T	Coalition	Google/Apple	MILA
Traçage par Bluetooth	Oui	Oui	Oui	Oui	Oui
Traçage par GPS	Non	Non	Oui (pour la localisation approximative)	Non	Oui
Collecte de données sur les contacts	Décentralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Chiffrement des données sur les contacts	Décentralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Production des clés secrètes des contacts	Centralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Stockage des données sur les contacts	Centralisé	Centralisé	Centralisé	s. o.	Centralisé
Évaluation du risque d'infection	Centralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Échange des données sur les contacts lorsqu'ils sont déclarés positifs	Envoi des clés des autres contacts	Envoi des clés des autres contacts	Envoi des clés des autres contacts	Envoi de ses propres clés de contacts	Envoi de ses propres clés de contacts Envoi de la localisation brouillée
Échange des données sur les contacts au moment de l'évaluation du risque d'infection	Envoi de ses propres clés de contacts	Téléchargement des clés des contacts des utilisateurs infectés	Téléchargement des clés des contacts des utilisateurs infectés	s. o.	Téléchargement des clés des contacts des utilisateurs infectés
Collecte des données des utilisateurs privés	Non	Non	Localisation approximative	Non	Oui
Système prédictif	Non	Non	Non	Non	Oui
Système potentiellement transfrontalier	Oui	Oui	Oui	s. o.	Non
Utilisation possible à d'autres fins que le traçage de contacts	Non	Non	Non	Non	Oui
Authentification humaine requise lorsqu'une personne est déclarée positive	Possiblement	Possiblement	Non	s. o.	Oui
Complexité relative de l'infrastructure du serveur (1 : de base à 5 : complexe)	2	3	3	s. o.	5
Open source	Partiellement en source ouverte (protocole + modèle de données)	Oui (kit de développement de logiciels pour appareils mobiles et serveurs)	Oui (*mobile library*)	À déterminer	À déterminer
Organisation	Gouvernemental	À but non lucratif	À but non lucratif	À déterminer	À but non lucratif

[60] 'Optic - Gouverner La Technologie En Temps de Crise', n.d., http://optictechnology.org/index.php/fr/news-fr/237-gouverner-la-technologie-en-temps-de-crise.

3.4. Légitimité et encadrement légal

Parmi les applications de traçage, certaines sont officiellement soutenues par le gouvernement local et peuvent être imposées ou recommandées.

La légitimité d'une application a pour condition le soutien et la promotion active du gouvernement. C'est un gage de réussite car cela peut conduire à une bonne adhésion et une bonne participation de la part du public, et c'est aussi un facteur important d'efficacité puisqu'une application de traçage n'a un véritable intérêt que si elle est correctement intégrée aux efforts généraux et à la stratégie globale des autorités sanitaires.

Dans certain cas, une législation spéciale est mise en place par les autorités pour encadrer le déploiement et l'utilisation de ces outils. Souvent, la gestion des données personnelles des applications de traçage s'inscrit dans un contexte légal plus large, comme par exemple le RGPD commun à l'ensemble de l'union européenne et qui s'applique aussi de manière extraterritoriale.

Enfin, ces outils peuvent avoir fait l'objet d'audits ou d'études d'impact sur la vie privée et les données personnelles avant d'avoir reçu le soutien du gouvernement.

En France, c'est à la fois le RGPD et la Loi Informatique et libertés qui s'appliquent. La Commission Nationale de l'Informatique et des Libertés (CNIL), créée à la suite du texte de loi éponyme, veille à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien dans les sphères publique et privée. En plus de son rôle d'observation, d'information, et de consultation, la CNIL dispose aussi de pouvoirs de contrôle et de sanction.

Dans le cadre du développement et du déploiement de l'application Stopcovid (StopCovid, StopCovid France), la CNIL a procédé à plusieurs contrôles afin d'évaluer la conformité de l'outil aux exigences de protection de la vie privée et des données personnelles de ses utilisateurs. Pour donner suite à ses évaluations, la CNIL a formulé des recommandations successives que le ministère des Solidarités et de la Santé devait intégrer. Ces recommandations[61] concernaient non seulement le fonctionnement propre de l'application vis-à-vis des législations encadrant les données personnelles, mais aussi sur la manière dont l'application s'inscrivait et contribuait à la stratégie du gouvernement pour contrer la pandémie.

> « Au regard des manquements constatés, le ministère des Solidarités et de la Santé a donc été mis en demeure de mettre l'application Stopcovid en conformité dans le délai d'un mois sur ces différents points. Il est également invité à engager dans les meilleurs délais une démarche d'évaluation du dispositif sur la contribution de l'application Stopcovid à la stratégie sanitaire globale et à rendre compte régulièrement de ses résultats à la CNIL. »

Le déploiement de l'application Stopcovid a été mis en œuvre après l'adoption d'un décret[62] visant notamment à préciser les conditions d'utilisation des données personnelles des usagers.

[61] 'Application « StopCovid » : La CNIL Tire Les Conséquences de Ses Contrôles | CNIL', n.d., https://www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles.

[62] 'Décret N° 2020-650 Du 29 Mai 2020 Relatif Au Traitement de Données Dénommé « StopCovid » - Légifrance' (n.d.), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041936881/.

4. Cartographie – Carte heuristique des applications de traçage

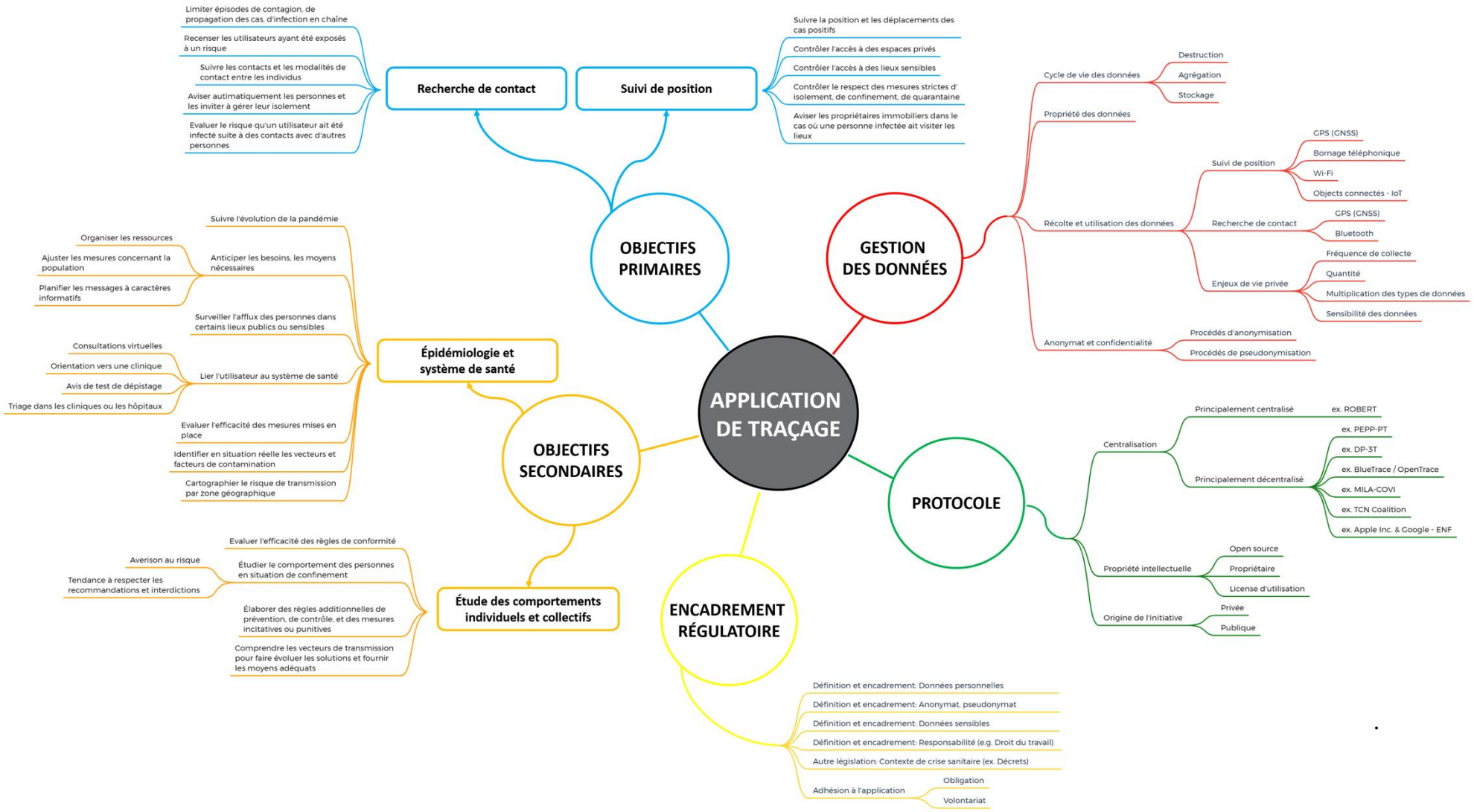

Illustration 5. Carte heuristique des applications de traçage

5. Conclusion

La pandémie du COVID-19 a plongé le monde dans un contexte inédit, non seulement du fait de son ampleur et de la paralysie des activités qu'elle a provoqué à l'échelle planétaire, mais aussi du fait de l'utilisation à grande échelle de nouvelles solutions technologiques visant à endiguer la propagation du virus et faciliter le retour à une vie quotidienne normale.

Parmi ces solutions technologiques, les applications de notification d'exposition représentent un cas particulier. D'abord, ces applications sont installées sur les téléphones intelligents et ont par conséquent pour support un outil qui fait partie intégrante de la vie quotidienne d'une grande partie de la population. Ces appareils sont tantôt une ombre de nous-mêmes, tantôt une extension de notre identité. Ensuite, ces applications représentent une solution singulière dans le sens où l'acte d'installation et d'utilisation confère à l'utilisateur une forme d'autonomie et de responsabilité. Au-delà des mesures barrières, des tests de dépistage, et des recommandations gouvernementales, chacun a le pouvoir de gérer soi-même son exposition au risque et d'agir en conséquence. Parallèlement, le déploiement des applications de notification d'exposition a amené des questionnements sur leur efficacité en mettant en avant la notion de seuil de masse critique, c'est-à-dire la proportion de la population devant utiliser l'application pour que celle-ci ait un quelconque impact. L'usage de telles applications pourrait aussi conférer aux utilisateurs un faux sentiment de sécurité, né d'une certaine illusion du contrôle qu'ils pourraient exercer et renforcé par les idées d'un certain solutionnisme technologique. Alors les comportements des utilisateurs peuvent être en dissonance avec les faits : l'absence de notification n'est pas la garantie d'un risque zéro. Les personnes croisées au cours d'une journée peuvent être asymptomatiques et ne jamais se faire tester, ou simplement ne pas avoir installé l'application.

Au développement précipité de ces solutions technologiques a suivi une période plus réflexive, nourrie à la fois des premiers retours d'expérience en situation réelle et de démarches plus circonspectes de la part des gouvernements. Outre l'enjeu crucial d'efficacité et d'adoption de ces solutions technologiques, le débat public s'est aussi concentré sur les problématiques de données personnelles (risques pour la vie privée, l'anonymat, la sécurité des données) et de gouvernance (souveraineté, propriété, centralisation/décentralisation, autonomie).

Il existe une grande pluralité dans les applications de traçage qui ont été développées depuis le début de la pandémie de la COVID-19. Les applications diffèrent d'abord au niveau des objectifs poursuivis (la finalité de l'application) et les technologies sur lesquelles l'application se base. Les deux grandes catégories de finalité recherchée sont le traçage de contact d'une part, et le suivi de la position d'autre part. Le traçage de contact vise à construire et avoir à disposition un historique des contacts entre les utilisateurs de l'application. Les appareils des utilisateurs s'échangent des identifiants lorsqu'ils sont à proximité, élaborant *in fine* une arborescence détaillant les flux de propagation potentiel du virus. Lorsqu'une personne se révèle comme étant infectée à la suite d'un test de dépistage, alors tous les utilisateurs de l'application ayant été en contact prolongé avec cette personne sont avertis du risque encouru, et invités à prendre des mesures particulières (isolement,

test de dépistage). La recherche de contact s'effectue principalement via l'utilisation de la technologie Bluetooth permettant à des appareils d'établir un dialogue et d'apprécier la durée et la distance des contacts entre les utilisateurs des appareils (la poignée de main digitale, *digital handshake*). Le suivi de position vise à pister la localisation des utilisateurs, en particulier ceux qui ont été testés positifs, afin de s'assurer qu'ils ne mettent pas d'autres personnes en danger d'infection. Les applications de suivi de position reposent sur des technologies comme les procédés de géolocalisation et navigation par un système de satellites (GNSS, notamment le GPS) ou bien sur la présentation et l'enregistrement de codes d'identification (à l'instar des codes QR) à certains points d'intérêt (comme l'entrée de lieux publics).

Les applications de traçage diffèrent aussi dans la manière dont elles conçoivent la confidentialité et la gestion des données personnelles. Dans certains cas, l'installation et l'enregistrement de l'application implique une étape où l'utilisateur doit fournir des renseignements personnels comme par exemple son numéro de téléphone, son nom et son prénom, son code postal, d'autres identifiants comme un numéro de sécurité sociale ou un numéro d'assurance maladie. Parfois, le profil d'utilisation de l'application est directement synchronisé avec un profil général national regroupant l'ensemble de ces informations et bien d'autres. Ces informations sont recueillies dans le but de faciliter le travail des autorités de santé publique dans le cas où un risque important est déclaré, suite par exemple à un dépistage positif et des contacts prolongés avec d'autres individus. A l'inverse, d'autres applications ne requièrent pas le renseignement de ce type d'information pour installer et utiliser l'application, et pourraient simplement les demander (sans les exiger) à la suite d'un test de dépistage positif.

Un thème influent de discussion au sujet de la conception des applications de traçage est le choix entre des protocoles ayant une architecture centralisée ou décentralisée pour la gestion des données des utilisateurs. Cette discussion est souvent simplifiée par la dichotomie suivante : les architectures centralisée sont plus efficaces pour la réponse sanitaire (données mises en commun, véracité et vérification des données), mais présentent davantage de risque pour la sécurité des données rassemblées et pour la protection des renseignements personnels de manière générale ; à l'inverse les architectures décentralisées sont un gage de protection de la vie privée puisque seule des informations éphémères et cryptées sont enregistrées directement sur les appareils des utilisateurs tandis qu'aucune information n'est sauvegardée de manière centrale. En réalité cette classification ou division nette n'a pas lieu d'être puisque ce sont chacune des étapes de l'ensemble du processus de fonctionnement de ces applications qui peuvent être réalisées de manière locale ou centrale. Comprendre quelles sont ces étapes et de quelle manière elles sont accomplies permet tout de même de juger de l'orientation générale du fonctionnement de l'application, centralisée ou décentralisée. Outre les enjeux purement techniques, les enjeux sanitaires (capacité à efficacement contenir un épiphénomène de propagation), et les enjeux éthiques directement liés à la protection de la vie privée et des renseignements personnels, le choix de la centralisation ou de la décentralisation s'inscrit dans la problématique de perception et de facteur d'acceptabilité sociale, c'est-à-dire de l'opinion du public vis-à-vis de la manière dont la solution est implémentée. Cette opinion aura un impact sur l'adoption de la solution par le public.

La finalité, la technologie choisie, le protocole et l'orientation de l'architecture supportant le fonctionnement de l'application, ainsi que le modèle de gouvernance sont des éléments intrinsèquement liés les uns avec les autres. Pour répondre à la crise sanitaire et ses conséquences sur la société, la question de la meilleure stratégie à mettre en place est fondamentale et légitime. Le choix d'une stratégie, d'une ou plusieurs solutions technologiques employées de consort avec des mesures sanitaires, a d'importantes implications. Ce choix n'est pas neutre, et il convient d'être en mesure de pouvoir peser le pour et le contre de chaque solution envisageable, d'en évaluer les avantages et les inconvénients, de comprendre les bénéfices atteignables et les risques pris. Cette appréciation doit se faire à plusieurs niveaux suivant les résultats attendus et l'efficacité visée, la priorité des objectifs, le contexte juridique, l'acceptabilité sociale, et les considérations éthiques (confidentialité, volontariat ou obligation). Après de nombreux mois de règles strictes, de confinement et de déconfinement, de vagues successives, de recommandations sanitaires, l'emploi de technologies numériques comme les applications de traçage reste une solution dont il est difficile de mesurer l'impact et les bienfaits. Plusieurs pays ont déployé ces solutions avec des résultats parfois approximatifs, parfois décevants. Les chiffres probants sur le nombre d'utilisateurs réels (et non pas juste de téléchargements depuis le lancement) ou sur le taux d'utilisation effectif manquent souvent pour venir mettre en perspective les chiffres concernant les signalements qui ont été réalisés grâce à l'application. Les applications de traçage ne sont donc pas une panacée, et si elles amènent une solution technologique qui pourrait être utile, elles doivent être implémentées en complètement d'autres mesures sanitaires. Elles ne peuvent fonctionner qu'avec le support de moyens de dépistage efficaces et de l'accompagnement des personnes infectées. Elles ne peuvent d'elles-mêmes endiguer la propagation du virus à grande échelle. Enfin, leur efficacité dépend grandement du taux d'adoption de la population, ce dernier résultant de plusieurs facteurs comme la légitimité perçue de l'application, de la menace ressentie par la population, et de sa compréhension du fonctionnement de l'application et des enjeux éthiques que son utilisation soulève. Alors qu'une « seconde vague » s'amorce et qu'autour du monde les mesures sanitaires se durcissent à nouveau, les gouvernements et les institutions de santé publique déploient de nouveaux efforts pour susciter l'adhésion de la population aux applications de notification d'exposition dans le but de limiter la propagation de la COVID-19. En France par exemple il s'agit de repenser les campagnes de communication et l'intégration de l'application à une stratégie plus large[63]; tandis qu'au Québec c'est l'application de notification d'exposition développée au niveau fédéral qui est finalement rendue disponible[64].

[63] Société civile et parlement Comité de contrôle et de liaison, 'Pour Un Système d'information Au Service d'une Politique Cohérente de Lutte Contre l'épidémie', 15 Septembre 2020, https://solidarites-sante.gouv.fr/IMG/pdf/avis_du_ccl-covid_du_15_09_20._pour_un_systeme_d_information_au_service_d_une_politique_coherente_de_lutte_contre_l_epidemie.pdf.

[64] Gouvernement du Québec, 'Les Québécois invités à télécharger l'application Alerte COVID', n.d., https://www.quebec.ca/nouvelles/actualites/details/les-quebecois-invites-a-telecharger-lapplication-alerte-covid-1/.

Bibliographie

MIT Technology Review. 'A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them.', n.d. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

American Civil Liberties Union. 'ACLU Comment on Apple/Google COVID-19 Contact Tracing Effort', n.d. https://www.aclu.org/press-releases/aclu-comment-applegoogle-covid-19-contact-tracing-effort.

American Civil Liberties Union. 'ACLU White Paper: The Limits of Location Tracking in an Epidemic', n.d. https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic.

Albergotti, Reed. 'Apple and Google Launch Coronavirus Exposure Software'. *Washington Post*, n.d. https://www.washingtonpost.com/technology/2020/05/20/apple-google-api-launch/.

'Application « StopCovid » : La CNIL Tire Les Conséquences de Ses Contrôles | CNIL', n.d. https://www.cnil.fr/fr/application-stopcovid-la-cnil-tire-les-consequences-de-ses-controles.

Le Devoir. 'Attention à la surveillance technologique généralisée', n.d. https://www.ledevoir.com/opinion/idees/577688/attention-a-la-surveillance-technologique-generalisee.

Belgium Corona App Task Force. 'Coronalert: A Distributed Privacy-Friendly Contact Tracing App for Belgium', 5 August 2020. https://www.esat.kuleuven.be/cosic/sites/corona-app/wp-content/uploads/sites/8/2020/08/coronalert_belgium_description_v1_2.pdf.

Argenox. 'Bluetooth LE Chipset Guide 2019 and Beyond', n.d. https://www.argenox.com/library/bluetooth-low-energy/bluetooth-le-chipset-guide-2019/.

'Cadre de réflexion sur les enjeux éthiques liés à la pandémie de COVID-19', n.d., 18.

CAI. 'Pandémie, Vie Privée et Protection Des Renseignements Personnels', May 2020. https://www.cai.gouv.qc.ca/documents/CAI_document-reflexion_PRP_COVID-19_FR.pdf.

Commissariat à la protection de la vie privée du Canada. 'Cadre pour l'évaluation par le gouvernement du Canada des initiatives en réponse à la COVID-19 ayant une incidence importante sur la vie privée', 17 April 2020. 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/fw_covid/.

Commissariat à la protection de la vie privée du Canada. 'Ce qu'une adresse IP peut révéler à votre sujet', 22 May 2013. https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2013/ip_201305/.

Commissariat à la protection de la vie privée du Canada. 'La protection de la vie privée et l'éclosion de la COVID-19', 20 March 2020. 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/gd_covid_202003/.

CEST. 'Comité spécial - Enjeux éthiques liés à la pandémie de COVID-19'. Commission de l'éthique en science et en technologie, n.d. https://www.ethique.gouv.qc.ca/fr/publications/ethique-covid19/.

CEST. 'CONDITIONS D'ACCEPTABILITÉ ÉTHIQUE', April 2020. https://www.ethique.gouv.qc.ca/media/1329/cest-conditions-acceptabilite-ethique_v7.pdf.

Comité de contrôle et de liaison, Société civile et parlement. 'Pour Un Système d'information Au Service d'une Politique Cohérente de Lutte Contre l'épidémie', 15 September 2020. https://solidarites-

sante.gouv.fr/IMG/pdf/avis_du_ccl-covid_du_15_09_20._pour_un_systeme_d_information_au_service_d_une_politique_coherente_de_lutte_contre_l_epidemie.pdf.

Commissariat à la protection de la vie privée du. 'Priorités stratégiques liées à la vie privée du Commissariat 2015-2020 - Tracer un chemin vers une meilleure protection', 2015, 23.

Commission d'accès à l'information du Québec. 'Rétablir l'équilibre - Rapport Quinquennal 2016', September 2016. https://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf.

'Communication & Information Technology Regulatory Authority Security Policy for Running Electronic Applications According to The Corona Virus Emergency Services Plan (Koweit)', n.d. https://citra.gov.kw/sites/en/Pages/applications.aspx.

'COVID-19 : Protection Des Renseignements Personnels et Sécurité de l'information | Commission d'accès à l'information Du Québec', n.d. https://www.cai.gouv.qc.ca/pandemie-de-covid-19-protection-des-renseignements-personnels-et-securite-de-linformation/.

Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid » - Légifrance (n.d.). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041936881/.

Observatoire international sur les impacts sociétaux de l'IA et du numérique. 'Efficacité et enjeux sociétaux des apps de traçage de contacts', 27 April 2020. https://observatoire-ia.ulaval.ca/3674/.

Exposure Notifications: Helping fight COVID-19 - Google. 'Exposure Notifications: Helping Fight COVID-19 - Google', n.d. https://www.google.com/intl/en_us/covid19/exposurenotifications/.

'ExposureNotification | Apple Developer Documentation', n.d. https://developer.apple.com/documentation/exposurenotification.

Gouvernement du Québec. 'Les Québécois invités à télécharger l'application Alerte COVID', n.d. https://www.quebec.ca/nouvelles/actualites/details/les-quebecois-invites-a-telecharger-lapplication-alerte-covid-1/.

'GPS.Gov: GPS Accuracy', n.d. https://www.gps.gov/systems/gps/performance/accuracy/.

Howard, Brandon, and JH Bloomberg School of Public Health. 'Digital Solutions for COVID-19 Response - An Assessment of Digital Tools for Rapid Scale-up for Case Management and Contact Tracing'. Johns Hopkins Bloomberg School of Public Health, n.d. https://www.jhsph.edu/departments/international-health/news/johns-hopkins-researchers-publish-assessment-of-digital-solutions-for-covid-19-response-in-low-and-middle-income-countries.html.

INRIA. 'Du Protocole à l'application StopCovid'. INRIA, n.d. https://www.inria.fr/sites/default/files/2020-05/From%20protocole%20to%20application.pdf.

INRIA. 'Protocole ROBERT - Un Protocole de Suivi Des Contacts Rapprochés, Rigoureux et Respectueux de La Vie Privée.', n.d. https://www.inria.fr/sites/default/files/2020-04/Pr%C3%A9sentation%20du%20protocole%20Robert.pdf.

Federal Trade Commission. 'Keeping Up with the Online Advertising Industry', 21 April 2016. https://www.ftc.gov/news-events/blogs/business-blog/2016/04/keeping-online-advertising-industry.

'Les enjeux éthiques de l'utilisation d'une application mobile de traçage des contacts dans le cadre de la pandémie de COVID-19 au Québec', n.d., 78.

Centre de recherche en éthique. 'Les enjeux éthiques des applications anti-pandémie', 10 April 2020. http://www.lecre.umontreal.ca/les-enjeux-ethiques-des-applications-anti-pandemie/.

'Major Security Flaw Uncovered in Qatar's Contact Tracing App', n.d. https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/.

'MIT TR Covid Tracing Tracker - Articles', n.d. https://www.technologyreview.com/tag/covid-tracing-tracker/.

Google Docs. 'MIT TR Covid Tracing Tracker - Google Sheets', n.d. https://docs.google.com/spreadsheets/d/1ATaIASO8KtZMx__zJREoOvFh0nmB-sAqJ1-CjVRSCOw/edit?usp=embed_facebook.

Nouvelle, L'Usine. 'En quoi consiste le protocole Désiré, la troisième voie de l'Inria pour l'application StopCovid ?', 14 May 2020. https://www.usinenouvelle.com/editorial/en-quoi-consiste-le-protocole-desire-la-troisieme-voie-de-l-inria-pour-l-application-stopcovid.N964166.

Google Docs. 'OBVIA - Applications de traçage COVID-19', n.d. https://docs.google.com/spreadsheets/d/12283mTnvhRgVUk1QCCOcs1gZZn4TgWA837LdxVRb49k.

Google Docs. 'OBVIA - Solutions technologiques COVID-19', n.d. https://docs.google.com/spreadsheets/d/1zxUr-SfSxwFQFf2I4aKmX5b_jLToGUyfWEM0gcWQmHQ.

'Open-Source Project Corona-Warn-App – FAQ – An Encounter Has Been Reported, but the Risk Status Stays Green', n.d. https://www.coronawarn.app/en/faq/#encounter_but_green.

'Open-Source Project Corona-Warn-App – FAQ – What Were the Reasons for Favoring the Decentralized Approach to Exposure Tracing?', n.d. https://www.coronawarn.app/en/faq/#reasoning_decentralized.

'Optic - Élaboration et Gouvernance Des Solutions Technologiques Pour Une Sortie de Crise Sanitaire', n.d. http://optictechnology.org/index.php/fr/news-fr/225-elaboration-et-gouvernance-des-solutions-technologiques-pour-une-sortie-de-crise-sanitaire.

'Optic - Gouverner La Technologie En Temps de Crise', n.d. http://optictechnology.org/index.php/fr/news-fr/237-gouverner-la-technologie-en-temps-de-crise.

Observatoire international sur les impacts sociétaux de l'IA et du numérique. 'Petit guide sur les enjeux et opportunités des applications de notifications d'exposition à la COVID-19', n.d. https://observatoire-ia.ulaval.ca/qa_covid/.

Petitgrand, Cécile, Jean-Noel Nikiema, Aude Motulsky, Philippe Després, Catherine Régis, and Jean-Louis Denis. 'OBVIA, Pôle Santé durable - Veille sur les outils numerIA dans la gestion de la pandémie de COVID-19', June 2020. https://observatoire-ia.ulaval.ca/axe/sante-durable/.

Apple. 'Privacy-Preserving Contact Tracing - Apple and Google', n.d. https://www.apple.com/covid19/contacttracing.

'Projects Using Personal Data to Combat SARS-CoV-2 - GDPRhub', n.d. https://gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2#Centralized_contact_tracing_systems.

Federal Trade Commission. 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers', 1 March 2012. https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

'Règlement Général Sur La Protection Des Données (RGPD) - Règlement (UE) 2016/679 Du Parlement Européen et Du Conseil Du 27 Avril 2016 Relatif à La Protection Des Personnes Physiques à l'égard Du Traitement Des Données à Caractère Personnel et à La Libre Circulation de Ces Données, et Abrogeant La Directive 95/46/CE (Règlement Général Sur La Protection Des Données)', n.d. https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679.

Roca, Vincent, Nataliia Bielova, Antoine Boutet, Claude Castelluccia, Mathieu Cunche, Cédric Lauradoux, and Daniel Le Métayer. 'DESIRE: une Troisième Voie pour un Système Européen de Notification d'Exposition', n.d., 6.

Sweeney, Latanya. 'Simple Demographics Often Identify People Uniquely'. . . *Pittsburgh*, n.d., 34.

'TGI de Paris, Ordonnance de Référé Du 2 Août 2019', n.d. https://www.legalis.net/jurisprudences/tgi-de-paris-ordonnance-de-refere-du-2-aout-2019/.

Datatilsynet. 'The Norwegian Data Protection Authority Has Imposed a Temporary Ban on Smittestopp Contact Tracing Mobile Application', n.d. https://www.datatilsynet.no/en/news/2020/the-norwegian-data-protection-authority-has-imposed-a-temporary-ban-on-smittestopp-contact-tracing-mobile-application/.

Twitter. '« Veuillez respecter les distances de sécurité. » À #Nice, si vous entendez des voix, regardez en l'air. #Drone #SeptAHuit', 16 April 2020. https://twitter.com/7a8/status/1250818601621340163.