

BOÎTE À OUTILS POUR LES APPLIS RELATIVES À LA COVID-19

Comment **les législateurs, les décideurs, les développeurs d'applications, les opérateurs, les organismes publics demandeurs et la population** peuvent-ils participer à l'amélioration des mécanismes de contrôle et faire en sorte que les outils déployés pendant une pandémie sont adaptés et efficaces ?

Table des matières

Introduction	1
1.Recommandations pour les décideurs et les législateurs	3
Pour les applis de recherche de contacts	4
Pour tous les types d’applis relatives à la COVID	20
2.Recommandations pour les développeurs d’applications, les opérateurs et les organismes publics demandeurs	26
Pour les applis de recherche de contacts	27
Pour tous les types d’applis relatives à la COVID	32
Outils pour la mise en œuvre	36
Confidentialité et protection des données dès la conception pour les applis de recherche de contacts	37
Modèle de spécification logicielle	40
Modèle de carte de flux de données pour applis de passeport immunitaire	41
Modèle d’énoncé sur la protection des renseignements personnels pour les applis de recherche de contacts	42
Modèle d’étude d’impact sur la confidentialité et la protection des données	44

Introduction

La COVID-19 a incité les gouvernements du monde entier à appliquer des mesures allant des mesures épidémiologiques traditionnelles, telles que le port du masque obligatoire et la distanciation physique, à un nombre sans précédent de mesures technologiques, plus particulièrement des applis de recherche de contacts et de passeport immunitaire.

Le projet « COVID App Project » d'applis relatives à la COVID est une initiative en deux parties de la société civile qui découle d'une recherche sur les interventions propres à la COVID.

La phase 1 du projet portait sur l'utilisation d'applis de recherche de contacts au Brésil, en Colombie, en Inde, en Iran, au Liban et en Afrique du Sud jusqu'en juillet 2021, évaluait l'impact de leur utilisation du point de vue de leur efficacité quant à la santé publique, et analysait le détournement d'usage ainsi que les conséquences imprévues telles que l'accès limité à la société. Cet intérêt de recherche partagé a réuni six organismes de la société civile : « ALT Advisory » (Afrique du Sud), « Internet Democracy Project » (Projet pour la démocratie d'Internet, Inde), InternetLAB (Brésil), Karisma (Colombie), SMEX (Liban), et « United for Iran » (Unis pour l'Iran). AWO, une agence spécialisée dans les droits en matière de données, assurait le soutien à la coordination.¹

La phase 2 du projet intègre des applications technologiques développées depuis juillet 2021, principalement des « passeports immunitaires » (qui présentent soit le statut vaccinal, soit des résultats de tests, soit des certificats de rétablissement). Appuyée par l'examen technique d'un échantillon d'applis représentatif à l'échelle mondiale, cette étude traite des tendances mondiales en matière d'approches politiques, juridiques et techniques d'après l'examen et l'évaluation technique de 11 applis relatives à la COVID développée (ou commandées) principalement par les gouvernements, mais aussi par d'autres intervenants en Australie, au Bahreïn, au Chili, en Indonésie, en Israël, aux Pays-Bas, en Tunisie et en Australie-Occidentale.

Ces pays ont été sélectionnés de manière à représenter les différents continents et régions du monde et pour refléter les tendances principales observées au cours de la recherche. Les autres applis examinées sont celles développées avec ce que l'on pourrait considérer être un rayonnement international : « CommonPass » du Forum économique mondial et « Travel Pass » de l'Association du transport aérien international.

Le résultat de cette seconde phase comprend :

- « Applis relatives à la COVID-19 : rapport sur les tendances politiques, juridiques et techniques » (ci-après dénommé « Rapport sur les tendances »)² les conclusions et recommandations de la phase 2 sont présentées dans ce rapport. Il prend en considération les approches de conception et d'usage des applis du point de vue de

¹ Les résultats de la recherche de phase 1 peuvent être consultés ici: <https://www.awo.agency/latest/covid-19-app-project/>

² Peut être consulté ici : <https://awo.agency/files/Covid-Apps-Policy-Legal-Tech-Trends.pdf>

leur efficacité quant à la santé publique, le niveau de détournement d'usage ainsi que les conséquences imprévues pour les utilisateurs. Cette analyse sert à établir un ensemble de recommandations et de pratiques d'excellence afin que les parties prenantes concernées développent des pratiques de santé publique efficaces et durables.

- « Logiciels relatifs à la COVID-19 : rapport sur les risques d'entrave à la vie privée (2e partie) » (ci-après dénommé « Rapport technique »)³ ce rapport présente un examen technique approfondi des 11 applis sélectionnées en prenant en considération leur adoption de pratiques d'excellence en matière de protection des données, entre autres la confidentialité et la protection des données dès la conception ainsi que la minimisation des données. Il comprend aussi des recommandations sur les meilleurs moyens d'assurer l'efficacité et la sécurité des applis relatives à la COVID-19.
- La « Boîte à outils pour les applis relatives à la COVID-19 » (ci-après dénommé « Boîte à outils »)⁴ la Boîte à outils est rédigée d'après les conclusions et recommandations énoncées dans le Rapport technique et dans le Rapport sur les tendances. Elle adopte aussi les conclusions émises lors de la phase 1 du projet COVID par les six organismes de la société civile indiqués ci-dessus et s'en inspire. Globalement, l'on trouvera dans le document un ensemble complet de pratiques d'excellence et des indications faciles à comprendre, ainsi que des outils pour leur mise en œuvre par toutes les parties prenantes impliquées dans la lutte contre la pandémie ou préoccupées par de telles interventions : les législateurs, les décideurs, les développeurs d'applications, les opérateurs, les organismes publics demandeurs et la population.

Les recommandations présentées dans cette Boîte à outils sont axées sur les manières d'améliorer les mesures de lutte contre la pandémie pour assurer l'efficacité du point de vue de la santé publique. Elles visent aussi à fournir des conseils pratiques aux parties prenantes impliquées dans la lutte contre la pandémie afin de prévenir le détournement d'usage et les conséquences imprévues lors du déploiement d'outils technologiques. Si cette Boîte à outils offre de bonnes pratiques et des recommandations de référence, les parties prenantes pourraient choisir de la personnaliser afin de refléter et d'aborder toutes les situations supplémentaires propres à leur contexte.

Bien que ces recommandations soient divisées par parties prenantes directement impliquées (p. ex. Recommandations pour les décideurs et les législateurs), elles sont toutes pertinentes pour toutes les parties prenantes.

Se familiariser avec les tendances et recommandations présentées par la Boîte à outils pourrait profiter à la population pour la sensibiliser aux enjeux qui la concernent (p. ex. Que devrais-je surveiller dans la politique de confidentialité d'une appli relative à la COVID ?). Pour améliorer encore une telle sensibilisation, chacune des deux sections de cette Boîte à outils commence par un bref résumé à l'intention des utilisateurs finaux : son objectif est de clarifier les attentes que la population pourrait avoir envers les parties prenantes impliquées dans la

³ Peut être consulté ici : <https://awo.agency/files/Covid-19-Apps-Technical-Review-2022.pdf>

⁴ Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-en.pdf>

lutte contre la pandémie, y compris en ce qui concerne une approche fondée sur la proportionnalité, qui respecte leurs droits et garantit l'efficacité quant à la santé publique.

Pour assurer un rayonnement international, la Boîte à outils est proposée en huit autres langues :

- Arabe⁵
- Chinois simplifié⁶
- Espagnol⁷
- Français⁸
- Hindi⁹
- Persan¹⁰
- Portugais (Brésil)¹¹
- Russe¹²

⁵ Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-ar.pdf>

⁶ Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-zh.pdf>

⁷ Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-es.pdf>

⁸ Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-fr.pdf>

⁹ Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-hi.pdf>

¹⁰ Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-fa.pdf>

¹¹ Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-pr.pdf>

¹² Peut être consulté ici : <https://awo.agency/files/covid-app-toolkit-ru.pdf>

1. Recommandations pour les décideurs et les législateurs

À quoi la population pourrait-elle s'attendre de ces parties prenantes impliquées dans la lutte contre la pandémie et pourquoi ?

Les décideurs et les législateurs peuvent établir des politiques et des cadres juridiques fondées sur les consultations et recommandations pertinentes du milieu de la santé publique. Pour la population, il est important de savoir que l'établissement de tels cadres et dispositifs de protection veillerait à ce que les actions des décideurs et législateurs tendent à garantir l'efficacité quant à la santé publique, tout en adoptant une approche fondée sur la proportionnalité. Une telle approche mènerait à l'élaboration et la diffusion de dispositifs de protection efficaces pour ce qui est de la conception et de l'utilisation d'applis relatives à la COVID-19, pour garantir l'observation de pratiques d'excellence internationales qui respectent les droits des personnes. Dans la pratique, si une appli relative à la COVID est utilisée par un pays comme élément de lutte contre la pandémie, l'efficacité d'une telle appli quant à la santé publique deviendrait l'élément d'une stratégie plus générale et coordonnée contre la COVID-19, ce qui est essentiel pour prévenir les conséquences inattendues.

Les utilisateurs finaux d'applis relatives à la COVID-19, dont les communautés vulnérables telles que les réfugiés et les travailleurs migrants, doivent pouvoir conserver l'accès aux services vitaux. Pour garantir une stratégie globale de santé publique qui facilite la confiance et qui est accessible à la population tout en étant facilement comprise par cette dernière, les applis doivent faire partie d'une stratégie plus générale fondée sur des données probantes. Cela signifie que si des applis sont adoptées, il y a coordination entre les différentes composantes du gouvernement aux niveaux fédéral et local, d'après des normes techniques internationales, et que leur usage est combiné à des initiatives de dépistage et de traçage, ainsi qu'à des politiques sociales et de santé publique telles que la distanciation physique. L'usage clair et coordonné de l'appli devrait être combiné à une mobilisation des médias (sociaux) pour accroître la sensibilisation de la population et l'éduquer au sujet de l'appli.

Enfin, la population doit pouvoir faire confiance aux interventions du gouvernement, ce qui entraîne ce qui précède ainsi que la prévention du détournement d'usage et des conséquences inattendues. Cet objectif peut être atteint en développant et en mettant en œuvre des régimes juridiques appropriés, une utilisation des données et des ententes de partage des données transparentes, seulement pour appuyer la stratégie de santé publique et non pour atteindre d'autres objectifs politiques ou d'orientation. Cette confiance peut être renforcée en

garantissant l'application homogène des mesures de santé publique dans le pays, sous surveillance indépendante, et en créant des solutions de substitution non numériques ou en prévenant autrement de punir la non-utilisation des applis.

Pour les applis de recherche de contacts

Efficacité quant à la santé publique		
Tendance 1		
Des mesures technologiques et des applis de recherche de contacts sont déployées dans les pays où l'accès à Internet et à la technologie mobile est insuffisant ou inégal	Évaluation	De nombreux gouvernements ont adopté des mesures technologiques pour lutter contre la COVID-19 malgré des disparités préexistantes quant à l'accès à Internet et l'adoption de la technologie mobile. On ne saurait trop insister sur l'importance de ce problème dans la mesure où l'accès inégal à la technologie des téléphones intelligents peut empirer les inégalités existantes et susciter des préoccupations d'ordre éthique. De plus, en proposant des services de sécurité sociale principalement sur des plateformes en ligne, les communautés vulnérables plus susceptibles d'avoir un accès insuffisant à Internet et sans appareils mobiles pourraient être privées d'une assistance vitale.
	Recommandation	Les autorités nationales devraient maintenir l'accès aux services vitaux pour les populations vulnérables (particulièrement pour les réfugiés et les travailleurs migrants).

Comment mettre en œuvre la recommandation ?

- Les autorités nationales pourraient établir l'état de la situation quant à la distribution d'une infrastructure Internet essentielle dans leurs pays respectifs pour déterminer les domaines ayant besoin d'être développés.
- Des investissements dans l'infrastructure Internet essentielle pourraient être réalisés dans les zones déterminées comme ayant besoin d'être développées. Cela pourrait comprendre de subventionner les forfaits de téléphonie mobile, de fournir des points d'accès Wi-Fi gratuits et même des programmes d'habileté numérique.

Efficacité quant à la santé publique

Tendance 2

Les applis étaient souvent déconnectées de l'intervention plus générale en santé publique et leur taux d'adoption était faible	Évaluation	Le sort des applis de recherche de contacts est souvent étroitement lié au manque de coordination des interventions contre la pandémie aux niveaux national et local. Certaines applis étaient en grande partie déconnectées de la stratégie plutôt sporadique de santé publique, et les gouvernements n'ont pas priorisé l'utilisation efficace des données. Cela signifiait aussi que les applis et autres mesures technologiques ne répondaient pas aux besoins du système de santé publique, ce qui a été rendu particulièrement évident par le manque de partage de données entre les autorités gouvernementales centrales et locales. C'est pourquoi certains prétendent que l'adoption d'une appli de recherche de contacts était simplement, dans certains pays, un exercice permettant de cocher une case pour montrer que le gouvernement se lançait dans des interventions technologiques contre la pandémie.
	Recommandation	Les autorités nationales devraient développer une riposte gouvernementale unifiée contre la COVID-19 (ou autres pandémies), qui prend en compte les organismes gouvernementaux à la fois nationaux et locaux.
	Comment mettre en œuvre la recommandation ?	
	<ul style="list-style-type: none">□ Les autorités nationales pourraient intégrer les applis de recherche de contacts dans l'infrastructure plus générale de santé publique, de dépistage et de traçage. Les applis donnent les meilleurs résultats si elles sont utilisées conjointement avec des systèmes traditionnels de dépistage et de traçage, qui eux même dépendent d'une capacité de dépistage suffisante et du personnel suffisant des autorités sanitaires locales, régionales et nationales.□ Faire appel à des politiques fondées sur des données probantes pour garantir des interventions de santé publique proportionnelles et efficaces.	

Efficacité quant à la santé publique		
Tendance 3		
Plusieurs applis polyvalentes sont déployées	Évaluation	Dans de nombreux pays, des applis de recherche de contacts différentes ont proliféré. Plusieurs applis différentes aux fonctions variées ont été publiées, surtout si elles avaient été conçues par les collectivités locales. Plus particulièrement, les gouvernements de certains états ou provinces ont déployé des applis dont les fonctions dépassent la recherche de contacts, telles que la télésanté. Cela découlait parfois d'une coordination limitée entre les établissements et de systèmes de santé publique décentralisés. Dans certains pays, la gamme d'applis officielles de recherche de contacts relatives à la COVID-19 a peut-être dilué leur adoption globale.
	Recommandation	Les autorités nationales devraient développer une riposte gouvernementale unifiée contre la COVID-19 (ou autres pandémies), qui prend en compte les organismes gouvernementaux à la fois nationaux et locaux.
	Comment mettre en œuvre la recommandation ?	
	<input type="checkbox"/> Garantir une intervention coordonnée des entités gouvernementales et des autorités de santé publique.	

	<ul style="list-style-type: none"> □ L'adoption de pratiques d'excellence internationales pour les applis de recherche de contacts telles que l'API GAEN (notifications d'exposition Google Apple) aide à créer une infrastructure robuste.
--	--

Efficacité quant à la santé publique		
Tendance 4		
Un manque de confiance et de sensibilisation de la population affecte les applis de recherche de contacts	Évaluation	<p>L'adoption d'applis de recherche de contacts a été entravée soit par un manque de confiance soit par une faible sensibilisation de la population dans tous les pays examinés. Cela provenait en partie d'une mauvaise campagne promotionnelle sur l'appli, dont l'absence de communications précises et ciblées du gouvernement. De plus, certaines applis étaient la cible de préoccupations quant à la surveillance, la confidentialité et la protection des données ; entre autres, dans certains pays, des antécédents d'abus du pouvoir de surveillance par les organismes d'application de la loi et les services de renseignements, impactant les journalistes, les chefs de l'opposition, les juges, et les défenseurs des droits de la personne</p>
	Recommandation	<p>Les autorités nationales devraient améliorer la communication avec et par les organes médiatiques. Le contenu devrait être scientifique et présenté de façon professionnelle pour augmenter la sensibilisation et l'éducation de la population.</p>

	Comment mettre en œuvre la recommandation ?
	<ul style="list-style-type: none"> <li data-bbox="734 331 2029 507">□ Les applis de recherche de contacts ne peuvent contribuer de façon significative que si les gens connaissent leur existence, font confiance à l'appli et à l'utilisation des données des utilisateurs par tous les acteurs et parties prenantes impliqués.¹³ L'application de pratiques d'excellence internationales en développement d'applis prévient le détournement d'usage ou les fuites de données afin que la population soit davantage disposée à utiliser l'appli. <li data-bbox="734 555 2029 619">□ Sensibiliser les gens à l'existence de l'appli et en encourager l'utilisation par les différents paliers de gouvernement, les autorités de santé publique, les médias et le secteur privé.

¹³ Ces acteurs sont dénommés contrôleurs de données ou « maître du fichier » d'après les lois de protection des données. Voici comment ils sont définis : « ... toute personne physique ou morale qui, conformément à la législation nationale, est habilitée à décider du choix et de l'utilisation des données de caractère personnel, que ces données soient ou non collectées, enregistrées, traitées ou diffusées par ladite personne ou par un agent agissant en son nom ». L'Organisation de coopération et de développement économiques - OCDE (11 juillet 2013). Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (ci-après dénommée « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE »). Peut être consulté ici : <https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188>

Efficacité quant à la santé publique

Tendance 5

<p>Les solutions de substitution ont souvent un plus grand impact sur la santé publique que les applis de recherche de contacts</p>	<p>Évaluation</p>	<p>Bien que les applis de recherche de contacts attirent l'attention et suscitent le débat public, les mesures de substitution ont souvent une portée supérieure. Certains pays ont compté principalement sur le dépistage de masse, les tests ciblés et les mesures de confinement, ce qui implique la mobilisation du personnel de santé pour procéder au dépistage de millions de personnes. Les mesures nationales de confinement et de quarantaine semblaient aussi avoir un impact important pour endiguer la propagation de la COVID-19.</p>
	<p>Recommandation</p>	<p>Les autorités nationales devraient concevoir une riposte contre la pandémie qui n'est pas fondée sur la technologie, comme solution de substitution à une intervention technologique avec des applis.</p>
	<p>Comment mettre en œuvre la recommandation ?</p>	
		<ul style="list-style-type: none"> □ Renforcer la coopération et la coordination entre les secteurs publics et privés pour garantir la préparation des hôpitaux et intégrer les applis de recherche de contacts dans une stratégie plus générale de santé publique qui comprend le dépistage et le traçage, ainsi qu'un dépistage accessible. □ Faire en sorte que des politiques sociales sont mises en place, qui permettent aux gens (possiblement infectés) de suivre les mesures et directives, p. ex. prévenir la pauvreté liée à la pandémie en offrant un soutien financier pendant la quarantaine et l'isolement. □ Faire en sorte que la population ait accès aux équipements de protection individuelle (p. ex. des masques).

Détournement d'usage et conséquences imprévues

Tendance 1

**Recours limité aux lois d'urgence,
recours prolongé à des pouvoirs
extraordinaires**

Évaluation

Au cours de la période à l'étude, les pays ciblés n'ont pas tous déclaré une urgence nationale. Pour ceux qui l'ont fait, l'assise juridique sur laquelle reposait la mise en œuvre des diverses mesures découlait de dispositions précises dans la constitution ou le cadre juridique du pays. Cela signifie habituellement que sous certaines conditions et règles, des pouvoirs peuvent être exercés par l'État tout en dérogeant aux normes habituelles relatives aux droits de la personne.

Cependant, l'état d'urgence peut impacter négativement certaines communautés vulnérables, particulièrement si les mesures mises en œuvre renforcent et exacerbent les pratiques discriminatoires existantes. Les pays qui n'ont pas déclaré l'état d'urgence se sont appuyés sur des dispositions législatives ordinaires combinées à des pouvoirs extraordinaires. Cela diffère d'une déclaration d'état d'urgence dans la mesure où une législation antérieure sous-tend de tels pouvoirs, habituellement des lois relatives à la santé publique, ce qui permet la mise en œuvre de certaines mesures sans pour autant être lié à un type d'urgence. Cela pourrait ne pas toujours être conforme à des dispositions explicites de la constitution ou du cadre juridique, et pourrait par conséquent donner lieu à l'exercice de pouvoirs étendus sans mise en place de mécanismes de contrôle appropriés.

	Recommandations	<p>Les autorités nationales devraient adopter des mesures de santé publique grâce à des instruments juridiques adéquats qui prévoient des garanties efficaces des droits de la personne, même si ces mesures sont fondées sur une déclaration d'urgence légitime.</p> <p>Lors de crises à venir, les autorités nationales devraient procéder à des études d'impact sur les droits de la personne déterminantes pour le cadre juridique, entre autres des réflexions sur les états d'urgence et de catastrophe, et sur ce qui serait nécessaire et justifiable.</p> <p>Avec un processus semblable à celui conçu pour traiter les violations graves des droits de la personne, il convient d'envisager des mécanismes de transition qui évaluent l'héritage des pratiques et normes créées pendant la pandémie de COVID-19, et promeuvent la reddition de compte ainsi que la reconfiguration afin que le caractère exceptionnel ne perdure pas.</p>
	Comment mettre en œuvre les recommandations ?	
	<ul style="list-style-type: none"> □ Instaurer des lois et des politiques pour affronter une nouvelle vague de COVID-19 ou une nouvelle pandémie afin de limiter le besoin de recourir à l'état d'urgence. □ Si une réponse rapide exige un état d'urgence, il doit être accompagné d'une disposition de temporisation qui stipule que les nouvelles mesures de santé publique devraient être strictement limitées dans le temps. □ Procéder à des études d'impact des lois existantes (ou à venir) relatives à la santé publique sur les droits de la personne avant qu'il ne soit nécessaire d'appliquer ces lois. Les études d'impact sur les 	

droits de la personne doivent être menées de façon transparente pour garantir à la fois une vérification au préalable adéquate et la confiance de la population.^{14 14}

- Faire appel à des politiques fondées sur des données probantes pour garantir des interventions de santé publique proportionnelles et efficaces. Prévenir les états exceptionnels prolongés en faisant appel à des pratiques d'excellence internationales d'études de l'impact et des politiques, soutenues par une adoption et une surveillance démocratiques.

¹⁴ Des indications sur la manière d'effectuer une étude d'impact sur les droits de la personne sont offertes ici (en anglais) : <https://www.business-humanrights.org/fr/big-issues/un-guiding-principles-on-business-human-rights/human-rights-due-diligence-impact-assessment/>

Détournement d'usage et conséquences imprévues

Tendance 2

Les pays ont des régimes embryonnaires de protection des données, qui parfois ne sont pas appliqués

Évaluation

Pour ce qui est des conclusions de la phase 1, pendant la pandémie, soit des lois complètes de protection des données n'étaient pas encore en vigueur, soit elles étaient encore à l'étape du processus législatif, soit elles n'existaient simplement pas. En général, des régimes plus robustes de protection des données pourraient renforcer le mécanisme de surveillance dans les pays en question.

Recommandations

Les autorités nationales devraient accélérer le processus d'application des lois de protection des données avec les dispositions nécessaires pour couvrir toutes les applis relatives à la COVID et tous les outils informatiques.

Les gouvernements et leurs partenaires privés devraient garantir des cadres réglementaires et stratégiques fondés sur les droits et transparents, axés plus particulièrement sur le droit à la vie privée.

Les lois sur la protection des données devraient être examinées et harmonisées avec toute loi existante séparée de protection des données.

Comment mettre en œuvre les recommandations ?

- Adopter des cadres en matière de protection des données ou les élargir quant à l'utilisation des données lors d'intervention en cas de crise, sans entraîner de nouveaux risques.
- Concevoir un mécanisme robuste de surveillance avec une autorité indépendante de protection des données.

	<ul style="list-style-type: none"> □ Harmoniser les lois sur la protection des données avec les pays voisins et les aligner sur les pratiques d'excellence internationales.^{15 15} □ Pour ce qui est de l'adoption ou d'une meilleure application des lois sur la protection des données, les organisations non gouvernementales (ONG), les groupes de défense des droits de la personne et autres organismes devraient continuer à offrir du soutien aux gouvernements.
--	---

Détournement d'usage et conséquences imprévues		
Tendance 3		
Partage de données accru et non transparent entre autorités publiques	Évaluation	<p>Dans les gouvernements du monde entier, il est commun que les autorités publiques collectent et partagent des données dans le cadre des interventions contre la pandémie. La raison principale étant de faciliter et d'approuver les demandes de voyage intérieur alors que les mesures de quarantaine sont en vigueur. Cela implique de combiner les jeux de données préexistants, ainsi que ceux générés particulièrement pour la COVID-19. Cependant, l'absence de lois exhaustives de protection des données et autres contrôles réglementaires engendre un détournement de l'usage et des effets perniciose sur certaines communes vulnérables, en partageant des données personnelles sensibles avec les organismes d'application de la loi et en restreignant le déplacement de ceux pour qui il est habituellement impossible d'accéder aux plateformes en ligne pour</p>

¹⁵ Ces pratiques d'excellence internationales comprennent les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE et Le Règlement général sur la protection des données (RGPD) de l'UE qui peut être consulté ici : <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr>

		demander des autorisations de voyage.
	Recommandations	<p>Les autorités publiques et les organismes privés qui collaborent au traitement des données personnelles lors d'une pandémie devraient préparer des rapports d'incidence et les publier comme bon exercice de transparence active et de reddition de comptes.</p> <p>Toutes les applis devraient présenter des documents juridiques essentiels tels que des conditions générales d'utilisation et une politique de confidentialité ; ces documents devraient appartenir au domaine public.</p> <p>Offrir des renseignements clairs sur le type de données recueillies et dans quel but, l'emplacement et la durée de rétention des données, les personnes avec qui les données seront partagées et à quelles fins, ainsi que les protocoles de sécurité sous-jacents à toutes ces fonctions.</p> <p>Les politiques de confidentialité devraient indiquer toute application tierce ayant accès aux données personnelles.</p>
	Comment mettre en œuvre les recommandations ?	
	<input type="checkbox"/> Les ententes de partage des données doivent comprendre des dispositions de temporisation claires.	

- Veiller à ce que les données obtenues du secteur privé soient soumises aux lois sur la protection des données et à une vérification préalable, entre autres si elles sont achetées ou partagées volontairement.
- Définir et publier des conditions générales de partage des données, des politiques de confidentialité et des renseignements sur la nature des données qui seront utilisées, par qui et comment.
- Les politiques de confidentialité doivent être compréhensibles, globales et expliquer toute application tierce.

Outils pertinents pour la mise en œuvre

- Modèle d'énoncé sur la protection des renseignements personnels pour les applis de recherche de contacts

Détournement d'usage et conséquences imprévues

Tendance 4

Un manque de confiance et de sensibilisation de la population affecte les applis de recherche de contacts	Évaluation	L'adoption d'applis de recherche de contacts a été entravée soit par un manque de confiance soit par une faible sensibilisation de la population dans tous les pays examinés. Une mauvaise campagne promotionnelle sur l'appli en était en partie la cause, avec une absence de communications précises et ciblées du gouvernement, contribuant à une confusion de la population au sujet de certaines applis. De plus, certaines applis étaient la cible de préoccupations quant à la surveillance, la confidentialité et la protection des données.
	Recommandations	<p>Les autorités publiques devraient mener des activités de communication précises et ciblées qui fournissent des renseignements précis et opportuns sur la COVID-19. Le contenu fourni devrait être scientifique et professionnel pour augmenter la sensibilisation et l'éducation de la population, et par conséquent améliorer la réponse aux mesures et restrictions.</p> <p>Les autorités publiques devraient tenir régulièrement des processus de consultation transparents, démocratiques et scientifiques avec les membres de la société civile.</p>
Comment mettre en œuvre les recommandations ?		

- Les applis de recherche de contacts ne peuvent contribuer significativement à l'efficacité sur le plan de la santé publique que si elles sont largement adoptées par la population, ce qui demande sa confiance. L'observation de pratiques d'excellence internationales (p. ex. la minimisation des données et la spécification des finalités) et la prévention générale du détournement d'usage sont des éléments fondamentaux pour gagner et conserver la confiance de la population. Consultez le modèle de spécification logicielle plus loin dans cette Boîte à outils.

Détournement d'usage et conséquences imprévues

Tendance 5

Discrimination à l'égard des groupes marginalisés

Évaluation

Certains des pays examinés ont déployé des applis qui permettaient aux utilisateurs de signaler aux autorités publiques les personnes qui contreviennent au confinement, grâce à des fonctions de signalement des rassemblements de masse et des voyageurs interétats dans leur région. Cependant, cela peut avoir de graves conséquences pour les groupes marginalisés, car l'on demande à des membres de la société civile d'exercer une surveillance au nom de l'État, sans les engagements envers l'égalité auxquels les États doivent habituellement se conformer. L'on donnait par conséquent l'occasion aux utilisateurs de pénaliser injustement certains individus ou même des groupes entiers.

Alors que les mesures relatives à la COVID-19, particulièrement les mesures nationales de confinement et le contrôle rigoureux des frontières, impactent des populations entières, il est plus probable que les migrants et les réfugiés subissent de l'exclusion ou de la discrimination. Ce n'est pas toujours avec efficacité que l'on garantit aux communautés les plus vulnérables une bonne protection contre ces risques, comme constaté dans certains pays. Nombreux sont ceux et celles qui se butent à des restrictions de voyage, particulièrement quand l'autorisation de voyage ne peut être obtenue que sur des plateformes numériques. Restreints par les mesures nationales de confinement, certains et certaines éprouvent même des difficultés à se loger, comme constatées dans certains pays. La COVID-19 a aussi intensifié les défis que doivent relever la population rurale et les personnes faisant partie des secteurs informels de l'économie, dont, par exemple, l'approvisionnement insuffisant en eau et le surpeuplement. Cela s'ajoute au recours controversé à des camps de quarantaine où l'on gardait les migrants en isolement pendant des

		semaines sans tests de dépistage de la COVID-19, les privant de la possibilité de se mettre eux-mêmes en quarantaine.
	Recommandations	<p>Les autorités publiques devraient appliquer les mesures de santé publique uniformément dans le pays.</p> <p>Les autorités publiques devraient veiller à ce que les services aux populations vulnérables (telles que les migrants et les réfugiés) soient maintenus afin de garantir qu'elles puissent traverser les difficultés persistantes associées à la pandémie. Ces services comprennent l'accès aux soins de santé, l'assistance financière et l'éducation.</p> <p>Les autorités publiques devraient veiller à ce que personne ne soit pénalisé ni ne se voit refuser l'accès à un service public ou privé en raison de la non-utilisation d'applications relatives à la COVID.</p> <p>Les mesures de santé publique devraient s'appuyer sur une étude d'impact qui prend en compte les conséquences possibles que les mesures pourraient avoir sur les groupes vulnérables.</p>
	Comment mettre en œuvre les recommandations ?	
		<ul style="list-style-type: none"> <input type="checkbox"/> Ne pas encourager ni exiger que la population signale les contrevenants aux mesures relatives à la COVID, car c'est le rôle des autorités publiques. <input type="checkbox"/> Faire appliquer uniformément les mesures de santé publique dans le pays et mettre en place une surveillance indépendante de leur adoption, accompagnée de mécanismes de rectification. <input type="checkbox"/> Veiller à ce que les migrants et les réfugiés soient compris dans les politiques de santé publique, les mesures de sécurité sociale et autres systèmes de soutien. <input type="checkbox"/> Mettre en place des solutions de substitution papier (non numériques) aux applications de recherche de contacts pour les personnes sans téléphone intelligent ou qui ne souhaitent pas utiliser d'applications.

- | | |
|--|--|
| | <ul style="list-style-type: none">□ Veiller à la poursuite des demandes d’asile et à des logements salubres et sûrs, en prenant en compte des options novatrices telles que des séjours en hôtel (qui seraient autrement vides en raison de la crise).□ Les autorités publiques devraient procéder à des études d’impact sur les droits de la personne, qui tiennent aussi compte des impacts possibles sur les différents groupes vulnérables. |
|--|--|

Détournement d'usage et conséquences imprévues

Tendance 6

Répression des protestations

Évaluations

Dans certains pays examinés, l'aide limitée fournie par les gouvernements nationaux et les collectivités locales pour résoudre les problèmes causés par les confinements et autres mesures relatives à la COVID a donné lieu à des protestations. Dans certains cas, ceci a entraîné l'emploi d'une force disproportionnée par les forces de l'ordre pour réprimer les protestations, impactant aussi les enfants, les malades et les personnes âgées.

Lors d'un autre examen de pays, il est devenu évident que les protestations s'étaient intensifiées en réaction à une présumée mauvaise gestion de la crise économique au cours de la pandémie. Les protestations étaient aussi alimentées par le manque de soutien du gouvernement pendant les mesures nationales de confinement, accentuant le ralentissement économique que de nombreuses personnes subissent. Les affrontements des manifestants avec les forces de sécurité ont fait des victimes alors que les autorités tentaient de réprimer les protestations, entre autres pendant les mesures nationales de confinement.

Recommandations

Les gouvernements ne devraient pas utiliser les politiques anti-COVID comme prétexte pour intimider les dissidents politiques et sévir contre eux. Ces politiques ne devraient pas non plus être utilisées pour punir les dissidents emprisonnés.

Comment mettre en œuvre les recommandations ?

- Les politiques de santé publique et les mesures législatives doivent être fondées sur des données probantes et présenter les objectifs clairement définis de combattre la propagation de la COVID-19 et d'assurer la poursuite, autant que possible, de l'activité sociale et économique. Ces limites doivent permettre la pleine jouissance des droits fondamentaux.
- S'ils n'existent pas encore, des mécanismes de rectification devraient être adoptés et maintenus en cas de violation des droits fondamentaux lors d'une pandémie. S'ils existent, ils devraient être mis en œuvre avec efficacité.

Détournement d'usage et conséquences imprévues

Tendance 7

Les interventions technologiques de lutte contre la COVID-19 ont aggravé la fracture numérique et les inégalités	Évaluations	Pour ce qui est de l'accès à Internet et de l'utilisation de la technologie mobile, les disparités ont une incidence sur l'accès de tout un chacun à la société pendant la pandémie. Cela s'avère être un problème crucial dans la mesure où un accès inégal à de telles ressources peut aggraver les inégalités existantes et soulever des inquiétudes sur le plan éthique. De plus, en rendant les services de sécurité sociale accessibles principalement sur des plateformes en ligne, les communautés vulnérables, dont bon nombre n'ont pas d'accès convenable à Internet et peu d'appareils mobiles, pourraient être privées de services essentiels. Cependant, même si les plateformes sont physiquement accessibles, leur conception peut avoir des implications négatives qui n'affectent pas seulement les communautés vulnérables. Par exemple, certaines applis de recherche de contacts n'étaient proposées qu'en anglais malgré la quantité de langues locales parlées par les utilisateurs.
	Recommandations	Des documents numériques doivent être conçus et rendus accessibles. Ces documents doivent être clairs et pertinents, accompagnés d'une formation et d'outils qui couvrent l'utilisation de l'appli concernée tout en mettant en évidence les enjeux essentiels en matière de protection des

		<p>données. Des formations d'habileté numérique devraient être offertes aux employés du gouvernement, aux travailleurs de la santé en milieu communautaire et aux utilisateurs des applis.</p> <p>Les autorités publiques devraient concevoir des solutions de substitution non numériques pour les demandes de déplacement et l'inscription à la vaccination.</p>
	<p>Comment mettre en œuvre les recommandations ?</p>	
	<ul style="list-style-type: none"> □ Mettre en place des solutions de substitution papier (et non numériques) pour toutes les politiques et initiatives de lutte contre la COVID-19, entre autres la recherche de contacts, les applis de recherche de contacts et l'accès au système de sécurité sociale. □ Aborder le problème de l'éducation à distance qui désavantage les enfants dans les milieux où l'économie est précaire. □ Adopter des politiques et du financement pour empêcher que la fracture numérique ne crée un écart encore plus grand entre les enfants. 	

Efficacité quant à la santé publique		
Tendance 1		
	Évaluation	Les politiques et mesures qui tentent de pallier une urgence devraient se fonder sur une raison d'être solide pour assurer leur efficacité. Ainsi, dans le contexte de la pandémie de COVID-19, toute intervention de santé publique devrait être adaptée aux conditions propres au pays où à la région, fruit d'une recherche scientifique en la matière. C'est avec plus ou moins de succès que les gouvernements ont réussi à impliquer les autorités de santé publique et autres experts pertinents dans le processus décisionnel de lutte contre la pandémie de COVID-19.

Manque d'engagement avec des politiques fondées sur des données probantes

Recommandations

Les gouvernements devraient s'assurer de la mise en place d'une structure essentielle appropriée pour garantir que les mesures technologiques adoptées soient aussi efficaces que possible si la technologie fait partie des interventions contre la pandémie. Particulièrement dans le contexte des applis mobiles et autres services Web, l'infrastructure Internet devrait être conçue afin que l'accès à Internet soit suffisamment réparti dans la population pour soutenir l'utilisation du réseau nécessaire à de telles interventions.

Les mesures technologiques utilisées en cas d'urgence en santé publique devraient être le fruit d'une recherche scientifique en la matière pour faire en sorte que de telles mesures répondent efficacement à l'urgence.

Les autorités de santé publique et autres entités composées d'experts compétents devraient être suffisamment impliquées dans le processus décisionnel afin que les décideurs puissent s'assurer et démontrer que leurs interventions sont fondées sur des études en la matière et appropriées aux circonstances propres à l'urgence à laquelle ils répondent.

Comment mettre en œuvre les recommandations ?

- Les autorités nationales devraient déterminer l'état de la répartition de l'infrastructure Internet essentielle dans leur pays respectif pour repérer les régions où elle doit être améliorée.
- Pour les régions où elle doit être améliorée, l'infrastructure Internet essentielle devrait recevoir des investissements. Subventionner les forfaits de téléphonie mobile, mettre en place des points d'accès sans fil et même proposer des programmes d'habileté numérique pour faire partie de ces investissements.
- Avant de procéder au déploiement, les décideurs et les législateurs devraient confirmer avec les experts si la technologie est une valeur ajoutée importante dans la lutte contre la COVID-19 ou si elle entraîne trop de dommages collatéraux pour justifier son existence. Les résultats de telles

consultations pourraient être présentés sous la forme de recommandations et soumis au comité décideur mentionné ci-dessous. Dans tous les cas, ces recommandations devraient être rendues publiques sur des sources libres et ouvertes.

- Mettre en place un comité aux pouvoirs décisionnels composé du secteur indépendant de la santé publique (épidémiologistes), de spécialistes en technologie, de décideurs et d'autorités chargées de la protection des données. Faire en sorte que les décisions prises par le comité font l'objet d'un contrôle.

Efficacité quant à la santé publique

Tendance 2

Manque de la sensibilisation de la population à la recherche scientifique qui sous-tend les mesures de lutte contre la COVID	Évaluation	La COVID-19 s'est propagée rapidement dans le monde entier et a présenté un nouveau type de risque pour la plupart des gens. Il y a eu par conséquent beaucoup à apprendre à la fois pour les gouvernements et les citoyens, ce qui a exigé, particulièrement au début, de prendre des mesures avec des connaissances limitées. Dans plusieurs endroits, on a pu aussi constater une augmentation des théories de conspiration qui entourent la maladie. De plus en plus d'indices montrent que l'adoption de la distanciation physique, de la quarantaine et des appels à la vaccination est fortement influencée par des campagnes bien conçues de sensibilisation de la population. En nombre d'endroits, ces campagnes ont contribué à une adoption plus proactive des mesures de santé publique, à la production locale de masques et couvre-visages où l'on ne pouvait en trouver, et la volonté de se faire vacciner.
	Recommandation	Créer des « coalitions de volontaires » avec une large représentation de la société civile. Les campagnes de sensibilisation, à la fois en ligne et hors ligne, peuvent faciliter l'adoption des mesures de santé publique et prévenir la perte de confiance. Prendre en compte les différentes caractéristiques démocratiques, particulièrement celle des communautés marginalisées, et travailler avec des groupes de confiance qui appartiennent à ces communautés.
Comment mettre en œuvre la recommandation ?		

- Les partenariats d'interventions fondés sur la communauté peuvent augmenter efficacement la sensibilisation des groupes marginalisés.¹⁶

¹⁶ Consulter (en anglais) : <https://apps.who.int/iris/rest/bitstreams/1277158/retrieve>; <https://www.ajtmh.org/view/journals/tpmd/105/4/article-p879.xml>;
https://www.cdc.gov/pcd/issues/2020/20_0408.htm

Efficacité quant à la santé publique		
Tendance 3		
Manque d'efficacité des commandes publiques pendant la COVID-19	Évaluation	Certains cadres législatifs prévoient des versions accélérées du processus d'approvisionnement qui permettent aux gouvernements de se procurer les ressources nécessaires pour répondre rapidement et efficacement à l'urgence rencontrée. Cependant, une gamme de problèmes peut se présenter si des processus accélérés complets de commande publique ne sont pas en place ou suivis, dont des pénuries d'équipement essentiel.
	Recommandation	Établir des règles permanentes, et non ad hoc, de commande publique lors de situations d'urgence pour garantir un approvisionnement plus efficace en biens ou services. Cela pourrait être aussi jumelé à des ententes préalables d'achat pour se procurer rapidement les biens et services qui pourraient être nécessaires afin de régler la situation d'urgence en question.
	Comment mettre en œuvre la recommandation ?	
		<input type="checkbox"/> Déposer un projet de loi sur les marchés publics qui reflète les parties pertinentes de la Loi type de la CNUDCI sur la passation des marchés publics ou une autre norme internationale semblable, en prêtant une attention particulière aux dispositions relatives aux commandes publiques en cas de situation d'urgence extrême. Ces dispositions pourraient par exemple comprendre que :

	<ul style="list-style-type: none"> ● La sollicitation d'une source unique est permise s'il y existe un besoin urgent de le faire en raison d'un événement catastrophique impliquant qu'il ne serait pas réaliste de recourir à une autre méthode de passation de marché à cause des délais qui en découleraient (reflète l'Article 30.5 [b] de la CNUDCI). ● Des négociations devraient être engagées avec le fournisseur pour déterminer la proposition et le prix, à moins que de telles négociations ne soient possibles dans les circonstances de la passation du marché (reflète l'Article 52 de la CNUDCI). ● Dans les cas urgents, les biens et services peuvent être obtenus auprès de certains fournisseurs d'après les ententes conclues entre l'État et ses fournisseurs antérieurement à la situation urgente qui entraîne l'urgence.
--	--

Détournement d'usage et conséquences imprévues		
Tendance 1		
Manque de cadre législatif pour le déploiement et l'utilisation des applis relatives à la COVID	Évaluation	<p>Dans certains des pays examinés, les applis et mesures de lutte contre la COVID-19 ont souvent été déployées sans adopter de cadres législatifs pour réguler leur usage et permettre aux autorités nationales de concevoir et déployer des applis relatives à la COVID. Dans certains cas, aucune loi n'était adoptée pour couvrir le traitement des données personnelles exigé pour que les applis relatives à la COVID puissent fonctionner. À cause de ces lacunes législatives, la possibilité de détournement d'usage augmenta, ce qui signifiait que les autorités nationales pouvaient utiliser ces mesures et les données personnelles pour des raisons autres que la COVID-19.</p>

	Recommandation	Mettre en œuvre un cadre législatif complet comme base de l'élaboration des mesures qui font partie de l'intervention d'urgence. Une disposition devrait être prévue dans la constitution ou dans le système juridique du pays pour invoquer un état d'urgence qui, pour un temps limité, modifie les rôles des différents services de l'État pendant la situation d'urgence afin de maintenir une surveillance et des mesures de sécurité suffisantes pour protéger les droits individuels.
	Comment mettre en œuvre la recommandation ?	
	<ul style="list-style-type: none"> □ Déposer un projet de loi qui prévoit que : <ul style="list-style-type: none"> ● L'exécutif, le gouvernement peut déclarer un état d'urgence sous certaines conditions, en stipulant que la déclaration doit être approuvée par le corps législatif. ● Les corps législatif et judiciaire assurent la surveillance pendant la situation d'urgence. ● Le gouvernement ne peut adopter des mesures d'intervention relatives à la situation d'urgence déclarée que si la nature et la portée de ces mesures sont clairement indiquées. ● Les mesures d'interventions mises en œuvre pour répondre à la situation d'urgence sont conformes aux lois existantes, entre autres la loi sur la protection des données. ● Le gouvernement garantit que toute dérogation aux droits individuels qui existent dans son système juridique ou dans sa constitution satisfait aux critères de proportionnalité. ● Les mesures adoptées pour répondre à la situation d'urgence déclarée font l'objet d'un examen a posteriori et de l'approbation du corps législatif. ● L'état d'urgence et les mesures adoptées pour répondre à la situation d'urgence doivent se conformer à un délai strict, et toute prolongation faire l'objet d'une approbation ex ante par le corps législatif. 	

Détournement d'usage et conséquences imprévues

Tendance 2

Accès réduit ou inégal à la société

Évaluation

Parfois, en situation d'urgence de santé publique, les gouvernements adoptent des mesures qui pourraient entraîner une discrimination à l'égard de certains groupes. Dans le contexte de la pandémie de COVID-19, certaines mesures ont été rendues obligatoires malgré le fait que les ressources et le soutien étaient insuffisants pour que les gens puissent s'y conformer. Par exemple, certains pays ont exigé que la population soit vaccinée contre la COVID-19 avant de pouvoir accéder à des lieux ou de voyager, malgré le fait que l'accès au vaccin soit limité ou que de grandes couches de la population n'étaient pas encore vaccinées.

Recommandation

Lors d'une situation d'urgence de santé publique, les gouvernements devraient s'assurer que les mesures obligatoires de santé publique sont accompagnées des ressources nécessaires et que les services sont accessibles afin que la population puisse se conformer à ces mesures et que l'accès à la société ne leur est pas injustement refusé.

Comment mettre en œuvre la recommandation ?

- Faire en sorte que les exigences pour accéder à la société soient largement répandues dans la population, entre autres la vaccination, le dépistage et les solutions papier de substitution aux applis.
- Les centres de vaccination et de dépistage doivent être accessibles à la fois dans les zones urbaines et rurales, et les solutions papier ou non numériques de substitution aux applis doivent aussi être largement répandues.

2. Recommandations pour les développeurs d'applications, les opérateurs et les organismes publics demandeurs

À quoi la population pourrait-elle s'attendre de ces parties prenantes impliquées dans la lutte contre la pandémie et pourquoi ?

Il est important que la population sache que les développeurs et les opérateurs d'applications ainsi que les organismes publics qui commandent les applications relatives à la COVID-19 peuvent prendre certaines mesures pour garantir l'usage efficace et durable des applications. Ces mesures composées de choix de conception, de protections et d'actes procéduraux favorisent la confiance et le succès d'usage des applications relatives à la COVID-19 dans le cadre d'une stratégie plus générale de santé publique.

Dans la pratique, les caractéristiques techniques et le développement des applications relatives à la COVID ont une incidence sur la collecte et l'utilisation des données personnelles des utilisateurs et la jouissance des droits fondamentaux, dont le droit à la protection de la vie privée.

Par exemple, rendre le code de l'application accessible au public encourage la confiance de la société civile et de la population. L'adoption de principes de confidentialité et de protection des données personnelles dès la conception peut prévenir le détournement d'usage et autres conséquences imprévues, prévenant ainsi la perte de confiance et les dommages qui découleraient de la mise en place de l'application. Cela comprend aussi de restreindre l'utilisation de données superflues telles que les données de localisation, pour lesquelles il existe habituellement des solutions de substitution. Le traitement des données (personnelles) doit être clairement défini avec une attention particulière à l'objectif, à la sensibilité des données, au stockage, à la sécurité et aux limites de partage. Tout partage de données, particulièrement avec le secteur privé, doit jouer un rôle clair dans la stratégie de santé publique, avec peut-être une exception pour les données de recherche, surtout pour diriger de futures politiques de santé publique.

Tout en se conformant à ces cadres respectueux des droits, ces applications doivent aussi être à l'épreuve du vieillissement en anticipant de possibles fraudes. Le fonctionnement de l'application ne peut aussi être garanti que si les fraudes qui se produisent peuvent être réglées avec efficacité et transparence.

Efficacité quant à la santé publique		
Tendance 1		
Le code de toutes les applis n'est pas rendu accessible au public	Évaluation	Toutes les applis examinées présentaient des lacunes sur le plan de la transparence, bien que les différences soient importantes d'une appli à l'autre. Le code de seulement trois applis était accessible pour vérification. La plupart font appel au brouillage du code, à la réflexion et à d'autres techniques anti-examen afin qu'il soit difficile de déterminer ou de confirmer la présence de certains comportements de manière fiable. De telles mesures ont une incidence négative sur la confiance et s'écartent des recommandations internationales de transparence et d'ingénierie en matière de protection des données personnelles.
	Recommandation	Pour toutes les plateformes, rendre le code des applis relatives à la COVID libre et ouvert. Rendre accessibles publiquement et vérifiables les codes côté serveur invite à la collaboration des personnes intéressées. Elles peuvent vérifier si des failles sont présentes dans le code et lancer un système d'évaluation par les pairs.
	Comment mettre en œuvre la recommandation ?	
<input type="checkbox"/> Publier le code source sur GitHub ou sur un autre site Web ou plateforme semblable pour codes source ouverts.		

	<ul style="list-style-type: none"> □ Ne pas utiliser de technique de brouillage pour dissimuler ou déformer le code source, ce qui rend difficile une inspection indépendante du code.
--	---

Détournement d'usage et conséquences imprévues		
Tendance 1		
Déploiement de solutions technologiques en collaboration avec le secteur privé	Évaluation	Certains de ces partenariats se présentent sous la forme d'entente de partage des données. D'autres partenariats portaient sur l'aide de compagnies privées aux gouvernements pour mener des activités de surveillance. Un inconvénient important de ces partenariats est l'absence de vérifications réglementaires appropriées. De plus, aucun des pays examinés n'a adopté un cadre complet de protection des données, ce qui compromet d'autant plus la légitimité de ces partenariats public-privé, créant ainsi des possibilités de détournement d'usage et d'exercice déséquilibré du pouvoir.
	Recommandation	Encadrer clairement les pratiques de partage de données entre les différents organismes gouvernementaux et le secteur privé.
	Comment mettre en œuvre les recommandations ?	
	<ul style="list-style-type: none"> □ Consulter la spécification logicielle afin de déterminer si le partage de données est nécessaire au fonctionnement de l'appli ou du système. <li style="margin-left: 20px;">□ Créer des cartes de flux de données et des relevés d'opérations de traitement pour documenter les données partagées avec les organismes gouvernementaux, et à quelles fins. Pour un exemple 	

	<p>de ce qu'une telle documentation pourrait comprendre, consultez le modèle présenté ci-dessous dans « Outils pour la mise en œuvre ».</p> <ul style="list-style-type: none">□ Consulter des experts juridiques pour rédiger des clauses sur les données à partager avec les organismes gouvernementaux, les fins d'un tel partage et autres obligations pertinentes qui devraient s'y appliquer. Ces clauses devraient être comprises dans tout contrat de prestation de services entre le concepteur et le gouvernement.
Outils pertinents pour la mise en œuvre	
<ul style="list-style-type: none">● Modèle de spécification logicielle● Modèle de carte de flux de données pour applis de passeport immunitaire	

Détournement d'usage et conséquences imprévues

Tendance 2

La plupart des pays choisissent d'adopter des systèmes centralisés pour leurs applis de recherche de contacts

Évaluation

On peut soutenir que les systèmes centralisés se conforment moins au concept de confidentialité et protection des données dès la conception que les systèmes décentralisés. Dans un système centralisé, la majorité du traitement nécessaire est effectué dans un serveur central exploité par une autorité publique, ce qui rend les données personnelles sensibles plus accessibles à ses autorités. En revanche, dans un système décentralisé, la majorité du traitement est effectué sur l'appareil de l'utilisateur où les données personnelles les plus sensibles restent sur l'appareil, et seules des données pseudonymisées sont partagées avec d'autres appareils et avec le serveur central. C'est le cas pour les pays qui utilisent l'API GAEN.

Recommandation

Le développement d'applications devrait respecter un cadre de confidentialité et protection des données dès la conception.

Comment mettre en œuvre les recommandations ?

- Pour le processus de développement logiciel, adopter une spécification logicielle qui définit les fonctions proposées de l'appli relative à la COVID en se conformant aux obligations légales pertinentes ainsi qu'aux principes de confidentialité et protection des données. Consultez le modèle présenté ci-dessous dans « Outils pour la mise en œuvre ».
- Obtenir les conseils d'un expert tiers indépendant pour évaluer la protection des données ou les risques quant à la confidentialité et le respect de la vie privée des applis relatives à la COVID lors de leur développement, garantissant ainsi que les principes de confidentialité et de protection des données sont interprétés et mis en œuvre adéquatement à chaque étape du cycle de développement, avant que le déploiement n'ait lieu.

Outils pertinents pour la mise en œuvre

- Modèle de spécification logicielle

Détournement d'usage et conséquences imprévues

Tendance 3

Utilisation habituelle des données de localisation

Évaluation

La collecte des données de localisation permet aux autorités nationales de suivre les utilisateurs à la trace et d'effectuer une surveillance plus intrusive qui dépasse les besoins de santé publique. Cela est particulièrement préoccupant quand les données de localisation peuvent révéler « les habitudes des utilisateurs, l'adresse de leur domicile, des données sur leur lieu de travail et même leurs croyances religieuses (c.-à-d. leur lieu de culte) ».

Recommandations

Réduire au strict nécessaire la quantité de données recueillies, particulièrement les données personnelles et celles qui permettent d'identifier les utilisateurs ; éliminer aussi le besoin d'obtenir la position GPS.

Afin de protéger la vie privée, supprimer les demandes de données de localisation de toutes les applications de recherche de contacts.

Offrir une option claire et facile d'accès pour supprimer un compte et les renseignements dans l'appli, ainsi que sur le serveur.

Comment mettre en œuvre les recommandations ?

- Effectuer des examens réguliers du code pendant le processus de transformation du concept architectural en lignes de code.
- Impliquer des experts ou des spécialistes en protection des données et en vie privée pour

s'assurer que le fonctionnement de l'appli se conforme à la spécification logicielle qui comprend les prescriptions ou les principes légaux applicables.

Détournement d'usage et conséquences imprévues

Tendance 4

Usage courant des outils pour le traçage et les analyses	Évaluation	Le principe de confidentialité et protection des données dès la conception n'est pas complètement suivi pour ce qui est des trousseaux de développement logiciel (SDK) déployés dans les pays examinés. En particulier, l'utilisation de la bibliothèque Firebase de Google ou d'autres trousseaux SDK n'est pas énoncée clairement dans les politiques de confidentialité respectives. Ainsi, il est impossible de bien juger comment Firebase de Google est utilisée, plus précisément si elle se limite à une analyse de l'installation ou si elle est utilisée à des fins générales de traçage plus intrusives sur le plan de la vie privée.
	Recommandations	Offrir des renseignements clairs sur le type de données recueillies et dans quel but, l'emplacement et la durée de rétention des données, les personnes avec qui les données seront partagées et à quelles fins, ainsi que les protocoles de sécurité sous-jacents à toutes ces fonctions.

		Publier des politiques de confidentialité plus détaillées (rédigées dans toutes les langues locales) et nommer explicitement tout tiers qui a accès aux données.
	Comment mettre en œuvre les recommandations ?	
		<ul style="list-style-type: none"> □ Évaluer les tiers fournisseurs des trousseaux SDK et autres bibliothèques logicielles à utiliser dans les applis relatives à la COVID. Ces évaluations devraient comprendre un examen des politiques de confidentialité et autres documents sur la protection des données pertinents, ainsi qu'une inspection du code tiers importé dans l'espace de travail pour le développement de l'appli.

Efficacité quant à la santé publique		
Tendance 1		
Fraude pour obtenir des certificats relatifs à la COVID	Évaluation	Attribuables en partie à la mésinformation et aux conspirations entourant la COVID-19, des cas existent d'individus qui ont tenté d'obtenir des codes QR frauduleux de manière à accéder à des lieux ou à voyager. Dans certains pays, le nombre de cas de fraude s'élevait à des dizaines de milliers.
	Recommandations	<p>Anticiper les tentatives de fraude et s'assurer que toutes les parties impliquées sont approuvées adéquatement, dont les partenaires du secteur privé.</p> <p>Dans le cadre des principes de confidentialité et de protection des données dès la conception, permettre la suppression des certificats obtenus frauduleusement en s'assurant que ce processus est intégré de façon transparente dans l'énoncé sur la protection des renseignements personnels.</p>
	Comment mettre en œuvre les recommandations ?	
		<ul style="list-style-type: none"> □ Effectuer des tests de vérification pour s'assurer que le fonctionnement du système répond aux exigences. Ces tests devraient comprendre : des tests unitaires (ciblant les différentes fonctions et composantes système), des tests d'intégration (ciblant l'interaction entre les groupes de composantes), des tests du système (ciblant les portions terminées du système entier) et des

	tests d'acceptation (en mettant le système entre les mains d'utilisateurs sélectionnés, c.-à-d. tests alpha et bêta).
--	---

Détournement d'usage et conséquences imprévues

Tendance 1

Absence de confidentialité et de protection des données dès la conception dans les applis relatives à la COVID

Évaluation

C'est avec un succès qui varie de l'une à l'autre que les applis relatives à la COVID abordent la confidentialité et la protection des données dès la conception. Si ce concept n'est pas adopté, les utilisateurs pourraient subir des dommages de façon disproportionnée. De tels dommages pourraient souvent se traduire par des développeurs d'applis, mais aussi par les gouvernements qui demandent leurs services, qui manquent de faire respecter comme il convient les droits à la confidentialité et à la protection des données des individus. Certaines applis utilisent des trousseaux SDK qui traitent les données à des fins sans rapport avec l'objectif principal de l'appli (la santé publique) ou partagent les données avec des tiers. De plus, la plupart des développeurs d'application ne sont pas transparents quant aux trousseaux SDK tierces ou bibliothèques logicielles utilisées dans leurs applis, ou ils ne publient pas leur code source, et autrement le brouillent. Enfin, la majorité des applis relatives à la COVID est aussi déployée sans qu'une étude d'impact sur la confidentialité et la protection des données soit effectuée auparavant pour déterminer les risques sur le plan de la confidentialité ou de la protection des données, et pour les atténuer. Cependant, certains pays ont fait l'effort de fournir des directives de protection des données aux lieux desquels l'on exigeait de recueillir certaines données personnelles à des fins de recherche de contacts.

	Recommandations	<p>N'utiliser que des trousseaux SDK qui traitent les données personnelles nécessaires à l'objectif de l'appli (c.-à-d. la recherche de contacts ou l'affichage d'information sur la santé).</p> <p>Rédiger des énoncés sur la protection des renseignements personnels qui informent les utilisateurs des applis dans un langage clair et concis sur la manière dont leurs données sont recueillies et traitées, et présenter ces avis de façon conviviale.</p> <p>Rendre ouvert et libre le code source des applis afin de permettre une vérification indépendante des fonctions et des opérations de traitement des données de l'appli.</p> <p>Si les organisateurs d'un événement public traitent des données personnelles (par exemple avec une recherche de contacts à la fois numérique et manuelle), fournir des indications sur la manière de traiter ces données de façon responsable, propices à une bonne protection des données.</p> <p>Avant déploiement, effectuer des études d'impact sur la confidentialité ou la protection des données pour déterminer les risques quant à la confidentialité ou à la protection des données et préparer des mesures appropriées d'atténuation des risques détectés.</p>
Comment mettre en œuvre les recommandations ?		

- Obtenir les conseils d'un expert tiers indépendant pour évaluer la protection des données ou les risques quant à la confidentialité et le respect de la vie privée des applis relatives à la COVID lors de leur développement, garantissant ainsi que les principes de confidentialité et de protection des données sont interprétés et mis en œuvre adéquatement à chaque étape du cycle de développement, avant que le déploiement n'ait lieu.
- Pour le processus de développement logiciel, adopter une spécification logicielle qui définit les fonctions proposées de l'appli relative à la COVID en se conformant aux obligations légales pertinentes ainsi qu'aux principes de confidentialité et protection des données. Le modèle présenté ci-dessous dans « Outils pour la mise en œuvre » propose un exemple de ce qu'une telle documentation devrait comprendre.
- Évaluer les tiers fournisseurs des trousseaux SDK et autres bibliothèques logicielles à utiliser dans les applis relatives à la COVID. Ces évaluations devraient comprendre un examen des politiques de confidentialité et autres documents sur la protection des données pertinents, ainsi qu'une inspection du code tiers importé dans l'espace de travail pour le développement de l'appli.
- Rédiger des énoncés sur la protection des renseignements personnels complets accompagnés d'une forme abrégée de l'énoncé, à fournir aux utilisateurs la première fois qu'ils utilisent l'application et qui soit accessible par la suite. Consultez le modèle présenté ci-dessous dans « Outils pour la mise en œuvre ».
- Publier le code source sur GitHub ou sur un autre site Web ou plateforme semblable pour codes source ouverts.
- Ne pas utiliser de technique de brouillage pour dissimuler ou déformer le code source, ce qui rend difficile une inspection indépendante du code.
 - Rédiger des directives de protection des données destinées aux gestionnaires de lieux, indiquant (i) les données qu'ils devraient recueillir et pourquoi (ii) comment ces données devraient être

recueillies et stockées (iii) l'obligation d'assurer la confidentialité de ces données et (iv) que ces données ne devraient être partagées qu'avec certains tiers dans le cadre des objectifs de leur collecte.

- Utiliser le modèle présenté ci-dessous dans « Outils pour la mise en œuvre » comme point de départ de la protection des données ou de l'étude d'impact sur la confidentialité et la protection des données à effectuer lors du développement de l'appli.

Outils pertinents pour la mise en œuvre

- Documents du modèle de spécification logicielle
- Modèle d'énoncé sur la protection des renseignements personnels pour les applis de recherche de contacts
- Modèle d'étude d'impact sur la confidentialité et la protection des données

Détournement d'usage et conséquences imprévues

Tendance 2

Montée des partenariats public-privé et manque de transparence

Évaluation

Les gouvernements ont tendance à tirer parti de leurs relations avec les entités du secteur privé pour atteindre divers objectifs politiques. Il n'y a pas d'exception dans le cadre de la COVID-19 : de nombreux gouvernements choisissent d'utiliser le système GAEN (notifications d'exposition Google Apple) pour construire leurs applis de recherche numérique de contacts ; certains pays approchent les entreprises de télécommunications pour obtenir des données afin de créer des cartes de densité et suivre la propagation du virus ; des gouvernements installent aussi des systèmes de caméras pour surveiller le respect des règles de quarantaine, développant ainsi l'appareil de surveillance de l'État. Cependant, ces partenariats sont souvent entourés d'un voile de secret ou, dans le cas de la COVID-19, exploitent le contexte de situation d'urgence pour se soustraire aux contraintes réglementaires habituelles qui ont pour objectif de garantir la protection des droits.

Recommandation

Publier dans le domaine public les conditions du partenariat pour toutes les applis qui ont été conçues sous partenariat public-privé.

Comment mettre en œuvre les recommandations ?

- Les gouvernements devraient garantir la transparence des partenariats public-privé (p. ex. en faisant droit aux demandes d'accès à l'information).

Outils pour la mise en œuvre

On trouvera ci-dessous des modèles ainsi que des exemples de pratiques d'excellence pour faciliter la mise en œuvre de certaines des recommandations présentées dans la Boîte à outils pour les applis relatives à la COVID-19.

Confidentialité et protection des données dès la conception pour les applis de recherche de contacts

Cet exemple présente un modèle d'appli de recherche de contacts qui renforce la protection de la vie privée, qui génère son propre code QR que les utilisateurs peuvent présenter (en donnant leur consentement) pour entrer et sortir de Lieux enregistrés dans cette appli (« Lieux enregistrés »).

Ces applis ne devraient être conçues que pour faciliter l'inscription des entrées et sorties par les Lieux enregistrés, tout en protégeant la confidentialité et les données personnelles, ce qui implique que :

- a. L'appli traite le moins de données personnelles possible ;
- b. Les données personnelles sont chiffrées le plus possible et ne peuvent être déchiffrées que par l'Autorité de santé publique si un cas positif de COVID a été détecté ;
- c. L'Autorité de santé publique ne reçoit que les données nécessaires pour trouver des personnes précises présentent dans un lieu public précis pendant une période donnée, alors qu'un risque de transmission de la COVID-19 a été détecté dans ce lieu ;
- d. Toutes les données d'entrée et de sortie sont supprimées dès qu'elles ne sont plus nécessaires à des fins de recherche de contacts, après 14 jours.

Accès aux données et leurs transferts

- Le développeur et l'opérateur de l'appli ne doivent accéder à aucune des données personnelles recueillies d'un utilisateur, traitées par les Lieux enregistrés et transférées à l'Autorité de santé publique.
- Les lieux qui utilisent l'appli pour inscrire les entrées et sorties des personnes n'ont qu'un accès strictement limité aux données personnelles, qui ne sont visibles qu'au point d'entrée pour faciliter les contrôles d'identité où cela est nécessaire. Seul le personnel autorisé du lieu a accès à ces données.
- L'Autorité de santé publique est autorisée à recevoir des données sur les personnes qui ont visité un lieu enregistré en même temps qu'une personne qui a reçu un diagnostic de COVID-19 (afin de pouvoir les contacter).

Fins déterminées

Les données personnelles peuvent être traitées afin de :

- a. Remettre un code QR aux personnes.
- b. Fournir au lieu un moyen sécurisé de recueillir les données de ceux et celles qui sont présents.
- c. Communiquer à l'Autorité de santé publique les données dont elle a besoin pour identifier et contacter les personnes qui pourraient s'être tenues à proximité de quelqu'un ayant reçu un diagnostic de COVID-19.

Données traitées

1. Sur les personnes qui utilisent l'appli :
 - a. Le nom, le prénom et l'année de naissance utilisés à des fins d'identification et de recherche de contacts.
 - b. Le numéro de téléphone mobile utilisé pour recevoir le code QR de l'appli et être contacté, le cas échéant, par l'Autorité de santé publique.
 - c. Dans le lieu, des cachets-codes QR d'entrée et de sortie, enregistrés dans l'appareil mobile d'une personne et sur les serveurs de l'appli, déchiffrés et utilisés à des fins de recherche en cas de communication des données par le lieu, à la suite d'une demande émanant de l'Autorité de santé publique.
2. Par les Lieux enregistrés
 - a. Adresse courriel, nom d'utilisateur, mot de passe du détenteur du compte, utilisés pour la création et la gestion du compte.
 - b. Nom, adresse courriel et numéro de téléphone de trois points de contact dans le lieu, utilisés par l'Autorité de santé publique pour remettre les demandes de communication des données à des fins de recherche de contacts.
3. Par l'Autorité de santé publique
 - a. Nom, prénom, année de naissance et numéro de téléphone mobile des personnes présentes dans un lieu précis pendant une période donnée, à des fins d'identification et de contact de ces personnes pour prévenir la propagation de la COVID-19.

Conservation et suppression des données

1. Personnes inscrites et codes QR :
 - a. Les données personnelles fournies à des fins d'inscription et de réception du code QR sont supprimées dès que la personne a reçu le lien vers le code QR.
 - b. Le code QR qui comprend les données personnelles chiffrées au sujet de la personne est conservé en deux endroits :
 - i. Sur l'appareil de la personne afin de permettre la lecture par les lieux.
 - ii. Sur le serveur du développeur ou de l'opérateur de l'appli afin de permettre aux personnes de télécharger l'image grâce au lien reçu par texto.

- c. Les utilisateurs peuvent supprimer n'importe quand leur code QR et le lien entre leur code QR et eux-mêmes, bien que les inscriptions d'entrée et de sortie de ce code QR soient quand même conservées pendant 14 jours à des fins de recherche de contacts.
 - d. Tous les codes QR et les moyens de les déchiffrer seront supprimés si l'Autorité de santé publique annule l'obligation légale qui dicte aux lieux de recueillir les données d'entrées et de sorties.
2. Données sur les lieux et leurs visiteurs :
- a. Les données personnelles relatives à un lieu seront conservées jusqu'à ce que :
 - i. Le lieu désactive son compte (auquel cas les données sur le lieu et les données d'entrée et sortie qui y sont associées seront conservées pendant 14 jours à des fins de recherche de contacts avant suppression),
ou
 - ii. L'Autorité de santé publique annule l'obligation légale qui dicte aux lieux de recueillir les données d'entrée et de sortie et tous les comptes sont supprimés.
 - b. Les données d'entrée et de sortie des Lieux enregistrés sont automatiquement supprimées après 14 jours.
 - c. Les données communiquées à l'Autorité de santé publique pour la recherche de contacts sont traitées conformément aux réglementations, aux politiques et aux procédures nationales en vigueur.
3. Les données relatives aux textos sont supprimées par l'appli, et les systèmes de traitement qu'elle utilise pour envoyer les messages suppriment les données de leurs serveurs dès que les textos ont été envoyés.

Communication des données à l'Autorité de santé publique

1. Les données des personnes sont chiffrées dans leur code QR. Les données sont associées aux lieux visités quand ces derniers lisent leur code QR. L'Autorité de santé publique ne peut accéder aux données et les déchiffrer que si la recherche de contacts le requiert.
2. Au cas où quelqu'un ayant reçu un diagnostic de COVID-19 serait associé à un lieu, l'Autorité de santé publique peut demander à ce lieu de communiquer les renseignements sur les personnes présentes pendant la même période. Le lieu peut autoriser le transfert de données relatives aux personnes ciblées ou demander d'autres éléments de justification à l'Autorité de santé publique si cela est nécessaire pour valider la demande.
3. L'autorisation de communication ne permet à l'Autorité de santé publique que d'accéder aux données relatives aux personnes ciblées, celles présentes dans le lieu pendant la période indiquée.

Sécurité de l'information

1. La sécurité de l'information est obtenue par la séparation des données, par des contrôles d'accès robustes et par le chiffrement. Les fonctions, l'architecture et le code base de la sécurité de l'information ont été vérifiés par des informaticiens indépendants.

Témoins de connexion

1. Le site Web de l'appli ne déploie que les témoins suivants strictement nécessaires afin de faciliter la création du compte et garantir la sécurité des données :
 - a. « csrftoken » est utilisé pour protéger le service contre la falsification de requête intersites.
 - b. « sessionid » est utilisé pour la juste attribution par le serveur de sessions aux utilisateurs authentifiés avec accès au tableau de bord.

Modèle de spécification logicielle

La spécification logicielle est un document qui décrit toutes les exigences auxquelles l'appli ou le système développé devrait se conformer. Ce document peut comprendre à la fois des exigences techniques et des obligations légales. Voici l'exemple d'une section de spécification logicielle qui définit une obligation légale qu'une appli de recherche de contacts devrait mettre en œuvre.

ID de l'exigence	EXIG-31
Énoncé de l'exigence	L'application devra utiliser le cadre de notifications d'exposition Google Apple pour le modèle de recherche de contacts
Auteur	[Nom]
Révision	1.1
Date de publication	[Date]
Mots-clés	Recherche décentralisée de contacts, minimisation des données
Obligation légale	<i>Principe de limitation de la collecte des FIPP (principes des pratiques équitables de traitement de l'information) : des limites devraient s'appliquer à la collecte de données personnelles et les données devraient être obtenues de façon honnête et licite quand cela est approprié, après en avoir informé la personne concernée ou avec son consentement.</i>

Description du scénario

Les applis qui utilisent le système GAEN génèrent des identifiants (ID) aléatoires (jetons cryptographiques appelés identifiants perpétuels de proximité) qui changent toutes les 10 à 20 minutes pour refléter la position géographique de l'appareil. Quand l'appareil de l'utilisateur est en contact étroit avec un autre appareil sur lequel une appli utilise le système GAEN, les deux appareils échangent par Bluetooth leur ID aléatoire respectif et les enregistrent. Les utilisateurs saisissent aussi dans l'appli les résultats positifs de leur test de dépistage de la COVID-19, et une liste des ID aléatoires que leur appareil a enregistrés au cours des 14 derniers jours est communiquée à un serveur central exploité par une autorité publique. L'appareil mobile comparera alors régulièrement les ID aléatoires qu'il a enregistrés à une base de données d'ID aléatoires associés à un test positif de dépistage de la COVID-19. En cas de correspondance, l'appli signale alors à l'utilisateur une exposition possible à quelqu'un atteint par la COVID-19 et lui conseille de suivre les directives de l'autorité publique compétente, par exemple effectuer un test de dépistage de la COVID-19 et s'isoler pour une période donnée.

Hypothèses de conception

Sur l'appareil, les jetons cryptographiques sont changés régulièrement d'après la position géographique de l'appareil.

Le serveur central exploité par l'autorité publique ne conserve que des données personnelles pseudonymes des utilisateurs (ID cryptographiques aléatoires).

Modèle de carte de flux de données pour applis de passeport immunitaire

On peut utiliser une carte de flux de données pour connecter les obligations légales à des étapes précises du cycle de vie des données afin de garantir que ses obligations sont pleinement respectées lors de la collecte et du traitement des données. Voici un exemple de carte de données qui énonce les obligations légales précises applicables à chaque étape du cycle de vie des données avec la fonction appropriée que l'appli devrait avoir par conséquent. Comme présenté dans l'exemple ci-dessus, l'ID d'exigence devrait correspondre à l'ID indiqué dans la signification logicielle concernée.

Cycle des données des renseignements sur la santé des utilisateurs		
Étape du cycle de vie des données	ID de l'exigence	Énoncé de l'exigence
Collecte	EXIG-51	L'application traite le statut vaccinal de l'utilisateur contre la COVID-19, les résultats des tests de dépistage de la COVID-19 et les renseignements sur l'immunité naturelle contre la COVID-19. Ces renseignements sur la santé seront recueillis lors de l'inscription et par la suite quand l'utilisateur saisira les renseignements dans l'application.
Usage	EXIG-78	L'application convertit les renseignements sur la santé de l'utilisateur en code QR que l'utilisateur peut montrer aux organisateurs du lieu afin de pouvoir y entrer.
Communication des données	EXIG-09	Le code QR de l'utilisateur sera généré afin que les exploitants du lieu puissent le lire.
Conservation	EXIG-12	Les renseignements sur la santé de l'utilisateur sont conservés tant que l'application est installée sur l'appareil de l'utilisateur. L'application ne conservera pas les données relatives à la position géographique où le code QR de l'utilisateur a été lu.
Destruction	EXIG-34	Les renseignements sur la santé de l'utilisateur sont détruits quand l'application est supprimée.

Modèle d'énoncé sur la protection des données personnelles pour les applis de recherche de contacts

Voici un exemple de forme abrégée d'énoncé sur la protection des renseignements personnels qui peut être utilisé pour les applis de recherche de contacts et présenté aux utilisateurs lors de leur inscription initiale sur l'appli. Le but est de présenter l'information la plus importante sur le traitement effectué par l'appli, avec la possibilité d'afficher l'énoncé complet ou d'envoyer une question au concepteur.

Your Privacy



This app was developed by Company A on behalf of Government 1.



When you use our app, we collect your name, address, phone number and health information. This health data includes for example your Covid-19 test results.



We use your data because it is necessary for the performance of a task carried out for public health purposes.



We collect your data when you first register on the app and as you continue to use the app.



We use your data to notify you if you have been in close contact with a person potentially infected with Covid-19.



We store your data in Country X and we use servers that are certified for health data hosting.



We use SDKs from the following third party providers:

- Provider 1
- Provider 2



This privacy notice was last updated on 1/1/22.

See Full Privacy Notice

Have a Question?



English Text	Translated Text
Your Privacy	La protection de vos renseignements personnels
This app was developed by [Company A] on behalf of [Government 1].	L'appli a été conçue par [entreprise A] au nom du [gouvernement 1].
When you use our app, we collect your name, address, phone number and health information. This health data includes for example your COVID-19 test results.	Quand vous utilisez notre appli, nous recueillons votre nom, votre adresse, votre numéro de téléphone et des renseignements sur votre santé. Ces données de santé comprennent par exemple les résultats de vos tests de dépistage de la COVID-19.
We use your data because it is necessary for the performance of a task carried out for public health purposes.	Nous utilisons vos données, car cela est nécessaire pour effectuer une tâche à des fins de santé publique.
We collect your data when you first register on the app and as you continue to use the app.	Nous recueillons vos données lors de votre inscription initiale dans l'appli et quand vous vous en servez.
We use your data to notify you if you have been in close contact with a person potentially infected with COVID-19.	Nous utilisons vos données pour vous signaler si vous avez été en contact étroit avec une personne qui pourrait être infectée par la COVID-19.
We store your data in [Country X] and we use servers that are certified for health data hosting.	Nous stockons vos données en/au/aux [pays X] et nous utilisons des serveurs certifiés pour héberger des données de santé.
We use SDKs from the following third party providers: <ul style="list-style-type: none"> ● [Provider 1] ● [Provider 2] 	Nous utilisons les trousseaux SDK des fournisseurs tiers suivants : <ul style="list-style-type: none"> ● [Fournisseur 1] ● [Fournisseur 2]
This privacy notice was last updated on 1/1/22.	La dernière révision de cet énoncé sur la protection des renseignements personnels a eu lieu le 1er janvier 2022.
See Full Privacy Notice	Consultez l'énoncé complet sur la protection des renseignements personnels
Have a Question?	Avez-vous une question ?

Modèle d'étude d'impact sur la confidentialité et la protection des données

Voici un modèle d'étude d'impact sur la confidentialité et la protection des données qui devrait être rempli avant qu'une appli soit déployée.

Système/Appli	[...]
Version du système, de l'appli	[...]
Date de l'ÉICPD	[...]

Contexte du projet de développement	
Quel est l'appli, le système que l'on développe ?	[...]
Pourquoi l'appli, le système est-il développé ?	[...]
Qui est impliqué dans le développement de l'appli, du système ?	[...]
Quelle sorte de tests ont été effectués sur l'appli, le système ?	[...]
Quelle est la date prévue du déploiement complet ?	[...]

Description de l'opération de traitement	
Quelles données personnelles sont utilisées par l'appli, le système ?	[...]
À quelles fins les données personnelles sont-elles utilisées ?	[...]
À qui les données personnelles sont-elles communiquées ?	[...]
Quelles trousseaux SDK ou autres bibliothèques logicielles tierces sont utilisées pour concevoir le système, l'appli ?	[...]

Identification des risques			
Menace	Vulnérabilité	Événement	Risque
[...]	[...]	[...]	[Faible, Moyen ou Élevé]

Gestion des risques			
Risque	Action	Type d'action	Justification
[...]	[Accepter, Transférer, Atténuer ou Éviter]	[Technique, Organisationnelle ou Contractuelle]	[...]