



APDPL

Association pour la Protection des Données au Luxembourg



WEBINAR : LES APPLICATIONS DE TRAÇAGE COVID-19 ET VOS DONNÉES PERSONNELLES

22 OCTOBRE 2020



INTERVENANTS



Emma
GOODWIN



Me Renaud LE
SQUEREN

- **L'application Covid au niveau français**
- **Les alternatives aux applications**
- **L'application Covid au niveau européen**

L'APPLICATION STOP COVID EN FRANCE





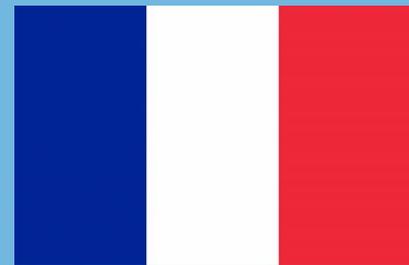
L'APPLICATION STOPCOVID EN FRANCE



- **Qu'est-ce que c'est ?**

- ✓ permettait de prévenir les personnes qui étaient à proximité d'une personne testée positive
- ✓ Temporaire
- ✓ reposait sur le volontariat
- ✓ se fondait sur la technologie Bluetooth
- ✓ Utilisait des données anonymisées

→ Développée par IRIA (*Institut national de Recherche en Informatique et en Automatique*) en collaboration avec Orange et Capgemini.





L'APPLICATION STOPCOVID EN FRANCE



- Comment cela fonctionnait ?

- ✓ L'application prévenait lorsqu'une personne a été en contact avec une personne affectée.
- ✓ Contact StopCovid = moins d'1m pendant plus de 15 minutes.
- ✓ Il fallait que les 2 personnes utilisent l'application.

- Diffèrent du « tracing » ?

- ✓ Utilisait la capacité à identifier les téléphones à proximité à partir des technologies Bluetooth et non les déplacements des personnes.

→ Problème avec Android qui n'a pas la capacité d'activer le Bluetooth sans activer le positionnement !





L'APPLICATION STOPCOVID EN FRANCE



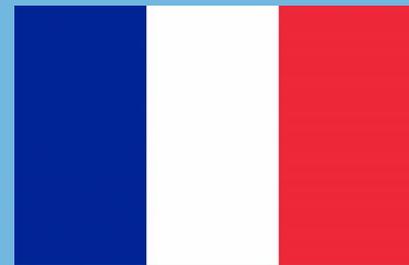
- Comment mes données étaient-elles stockées?

La France misait sur une approche « **centralisée** » : les données, non nominatives, devaient être stockées sur des serveurs centraux et contrôlés par les autorités sanitaires.

Une autre approche « **décentralisée** » prévoyait que les informations-clés, nécessaires au fonctionnement du service, seraient stockées directement sur les smartphones des utilisateurs et circulent entre eux lorsque c'est nécessaire.

→ Le gouvernement a choisi l'approche centralisée.

→ La CNIL recommandait que les données soient stockées sur le territoire de l'UE seulement.





L'APPLICATION STOPCOVID EN FRANCE

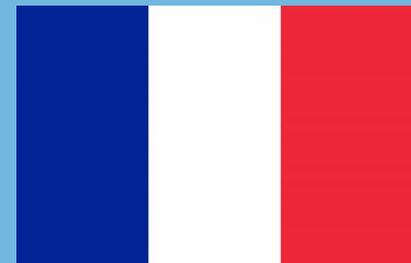


- **Combien de temps l'application gardait mes données ?**

- ✓ Les données liées à la mise en œuvre de l'application (clés et identifiants associés aux applications) = **6 mois** à compter de la fin de l'état d'urgence sanitaire.
- ✓ Les données telles que les historiques de proximité des personnes diagnostiquées ou testées positives = **15 jours** (*Recommandation de Santé Publique France et du ministère chargé de la Santé*).

- **Transferts des données Hors EU via des sous-traitants ?**

- ✓ Les données n'étaient pas destinées à être transférées hors de l'UE (*Recommandation CNIL*).
 - ✓ Appel à certains sous-traitants dans le cadre de l'hébergement des données et la maintenance du système.
- L'accès aux données par les sous-traitants se faisaient uniquement pour le compte et sur les instructions du ministère en charge de la santé (*Responsable du Traitement*) .





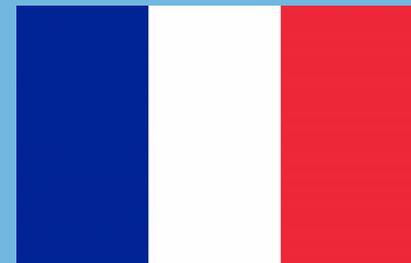
- Qu'est-ce qui n'a pas fonctionné ?

1. Contradiction avec le décret qui encadre l'utilisation de StopCovid

- ✓ Pour Gaëtan Leurant, chercheur en cryptographie à l'Inria, « StopCovid reposait sur la remontée de l'historique de proximité d'un utilisateur diagnostiqué positif : cet historique de proximité était constitué des contacts rencontrés par l'utilisateur positif ».

→ Sous-entendu : tous les contacts, et non pas seulement les plus proches ».

- Interrogé par Mediapart, Cédric O a **justifié cette pratique**. Ainsi, le secrétaire d'État a fait savoir que l'application utilisait tous les contacts et non pas uniquement les utilisateurs les plus proches.





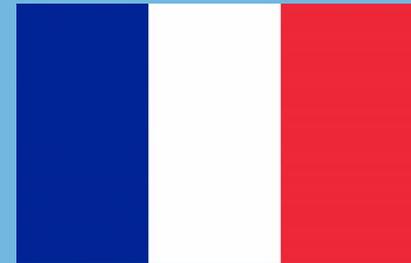
- Qu'est-ce qui n'a pas fonctionné ?

2. Efficacité d'une application sur base du volontariat

- ✓ « depuis le 2 juin, seules 2,3 millions de personnes ont téléchargé l'application StopCovid - soit à peine 3 % de la population française -, et seulement 72 notifications de contacts à risque ont été recensées. » - Directeur Général de la Santé
- pour que cette application ait été efficace, il aurait fallu que 60 à 70 % de la population l'utilise.

3. Limites des applications de traçages utilisant Bluetooth

- ✓ Concernant la géolocalisation via les antennes relais, « les données ne sont pas assez précises pour vous dire à quel point deux téléphones sont proches l'un de l'autre. » - American Civil Liberties Union*
- l'application ne pouvait pas tenir compte d'éventuels éléments séparant des personnes situées à proximité puisque le Bluetooth traverse les murs.





- Qu'est-ce qui n'a pas fonctionné ?

4. Incertitudes technologiques de l'application face à Apple et Google

- ✓ Apple et Google découragent les applications centralisées et **la diffusions en tâche de fond.**

→ Le Secrétaire d'Etat est d'avis que cette fonction est essentiel pour l'efficacité de l'application afin de faire la connexion entre les utilisateurs même quand l'application n'est pas ouverte.

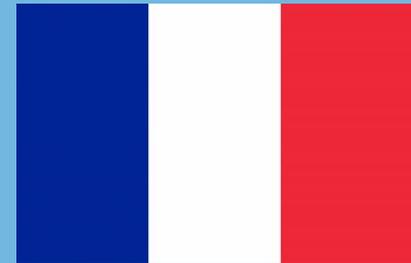
- ✓ Apple et Google n'ont **pas plié face au Gouvernement**, l'application devait être modifiée pour pouvoir être téléchargeable depuis l'App store/Google Play store.

→ Le Gouvernement a du contourner le problème = abandon des tâches de fonds en Bluetooth.

→ Faute d'utiliser l'APIE Exposure notification d'Apple et Google, Stopcovid était inopérante dans certains cas.



- Nouvelle Application en France : « TOUS ANTI COVID »
- ✓ Nouvelle application qui vient remplacer « StopCovid » prévue pour le 22 octobre.
- ✓ Objectif: rendre l'application **plus interactive** pour qu'elle soit plus téléchargée, tout en gardant la même base technique (toujours centralisée).
- ✓ Inclura des **informations générales**: comment circule le virus? Quels sont les gestes barrières? Où sont les points pour se faire tester (...)
- ✓ Disposera d'un **QR code** pour permettre aux utilisateurs de scanner les endroits où ils sont, tels qu'au restaurant par exemple.
- ✓ **Fonction météo** : L'utilisateur sera appelé à renseigner sa ville ou sa région afin d'accéder à un suivi plus précis de l'épidémie autour de lui.
→ ces données doivent être renseignées manuellement, **pas de fonction de géolocalisation**.



AUTRES MOYENS DE TRACING





AUTRES MOYENS DE TRACING



- **Registre papier**

À l'entrée de tous les lieux publics : obligation, par le Conseil National de Sécurité (CNS), pour les personnes de donner leur nom/prénom, adresse email et numéro de téléphone dans un **registre papier tenu par la personne responsable du lieu.**

Ces données sont détruites après **14 jours.**

Beaucoup de réactions négatives :

→ Le ministre des Indépendants et PME et la présidente de la fédération des cafés de Belgique ont estimé que cette mesure est **illégal** et constitue une atteinte à la vie privée des gens.





AUTRES MOYENS DE TRACING



- **CoronaAlert**

Lorsqu'un médecin prescrit un test, l'utilisateur reçoit un code qu'il peut lier au résultat de son test dans l'application. En cas de résultat positif, la personne le reçoit via l'application et peut notifier toute personne avec qui elle est entrée en contact.

Données anonymisées → permet de garder une trace anonyme des contacts.

Base de données **conservée par Sciensano** suite aux tests réalisés = Décentralisée

Différent de
la France

Utilise une technologie développée par Apple et Google, à savoir la **notification d'exposition**.

→ votre téléphone peut générer et partager du “charabia” anonyme. Ce “charabia” anonyme est partagé lorsque vous êtes en contact avec d'autres utilisateurs de l'application.

Les données stockées dans le téléphone de chaque utilisateur et dans le serveur central sont **automatiquement supprimées après 14 jours**.





AUTRES MOYENS DE TRACING



- **Corona-Warn-App**

- ✓ Décentralisée, sans point de contact avec une autorité médicale tant qu'on n'est pas infecté.
→ Le système décentralisé rencontre **davantage la confiance des citoyens**.
- ✓ Collaboration avec Google et Apple – **Notification d'exposition**
- ✓ Caractère **transfrontalier** (disponible: LU, BE, DK, RO, FR, Rep. Tchèque, Autriche et Bulgarie)
- ✓ Identifiants de proximité: stockés sur le smartphone et sont changés tous les 10 à 15 minutes (localisation impossible)
- ✓ En cas de résultat positifs: les codes collectés (contacts) sont stockés sur des serveurs cloud de Deutsche Telekom – données anonymisées qui ne permettent pas d'identifier ni la personne ni sa localisation.
- ✓ Les codes ne sont pas stockés plus de **14 jours** (durée limite d'incubation).





AUTRES MOYENS DE TRACING



- **Enquête CoviPrev :**

Objectif : vise à suivre l'évolution des comportements et l'adoption des mesures de protection (gestes barrières, confinement, etc.) des personnes.

Questionnaire auto-administré à remplir en ligne sur système Cawi (Computer Assisted Web Interview).

Surveillance qui permet de vérifier la connaissance des mesures de protection, ainsi que la santé mentale des personnes pendant l'épidémie Covid19.

Les résultats de cette étude sont publiés seulement sous forme de chiffre qui démontre l'évolution des symptômes, et l'épidémie. Aucune autre données n'est partagée.

<https://www.santepubliquefrance.fr/etudes-et-enquetes/covid-19-une-enquete-pour-suivre-l-evolution-des-comportements-et-de-la-sante-mentale-pendant-l-epidemie#block-242830>





AUTRES MOYENS DE TRACING



- Application MAELA à Luxembourg

Permet une **surveillance médicale** à distance de tous les patients dont les tests COVID ont été positifs :

La personne concernée est inscrite dans le système national directement (**pas sur base du volontariat**) par l'hôpital au moment de sa sortie ou par l'inspection sanitaire après avoir reçu les résultats positifs du laboratoire.

La personne concernée doit répondre tous les 2 jours à un questionnaire pendant 2 semaines pour évaluer l'état de santé du patient, identifier les besoins et éventuellement une prise en charge en cas d'aggravation de son état de santé.

<https://suivicovid.lu/>





AUTRES MOYENS DE TRACING



- Quelle est la position de la Commission Européenne ?

La Commission a donné son accord pour les applications de suivi des contacts, mais rejette la collecte de données de localisation incompatible avec le RGPD :

- ✓ Les chefs de projets doivent être soit des institutions soit des autorités publiques.
- ✓ Les applications doivent être sur **base volontaire, anonyme et au-delà des frontières nationales.**
- ✓ Pouvoir garantir que l'application sera automatiquement désactivée chez tous les utilisateurs dès que la crise sanitaire qui la justifie sera terminée.



L'APPLICATION COVID EN EUROPE



L'APPLICATION COVID AU NIVEAU EUROPÉEN

- Pourquoi utiliser un app ?
- Comment fonctionnent les applications de traçage ?
- Les applications décentralisées - Traitement, stockage et traçage à proximité
- Comparaison des différents états membres
- Implications RGPD/Directive ePrivacy
- La faiblesse des solutions
- Conclusion





L'APPLICATION COVID AU NIVEAU EUROPÉEN

- La Commission Européenne a reconnu que les applications de traçage satisfont aux quatre fonctions :
 1. Donner des informations et conseils aux citoyens sur le Covid-19 et des mesures générales adoptés par des états membres.
 2. Fournir des questionnaires d'autoévaluation, contrôle de symptômes ou des fonctionnalités de télémédecine.
 3. Tracer des contacts pour informer des personnes à proximité d'un patient infecté
 4. Mettre à disposition un forum de communication entre des patients et des médecins qui sont en auto-confinement ou qui ont besoin d'une autre diagnostic ou des avis sur le traitement (usage augmenté de télémédecine).





L'APPLICATION COVID AU NIVEAU EUROPÉEN

Traitement et stockage des identifiants par DP-3T
(Decentralised Privacy-Preserving Proximity Tracing)

Bluetooth à basse énergie



Émission EphID

EphID

Stockage local
(EphID, mesure
du timing et
exposition)





L'APPLICATION COVID AU NIVEAU EUROPÉEN

Production et stockage des identifiants par DP-3T
(Decentralised Privacy-Preserving Proximity Tracing)

SK_t ← Le jour actuel t
↙
Clé secret

La même clé est rafraîchie chaque jour avec une fonction de hachage

$$SK_t = H(SK_{t-1})$$

Si la clé est compromise toutes les clés secrets ultérieures sont découvertes,
MAIS les clés secrets précédentes ne sont pas révélées.





L'APPLICATION COVID AU NIVEAU EUROPÉEN

Production et stockage des identifiants par DP-3T
(Decentralised Privacy-Preserving Proximity Tracing)

SK_t ← Le jour actuel t



Clé secret qui produit une série de EphID en utilisant une fonction PRF (pseudorandom function) et PRG (pseudorandom generator) – AES in counter mode)

$EphID_1 \mid \mid \dots \mid \mid EphID_n = PRG (PRF(SK_t, \text{« clé d'émission »}))$

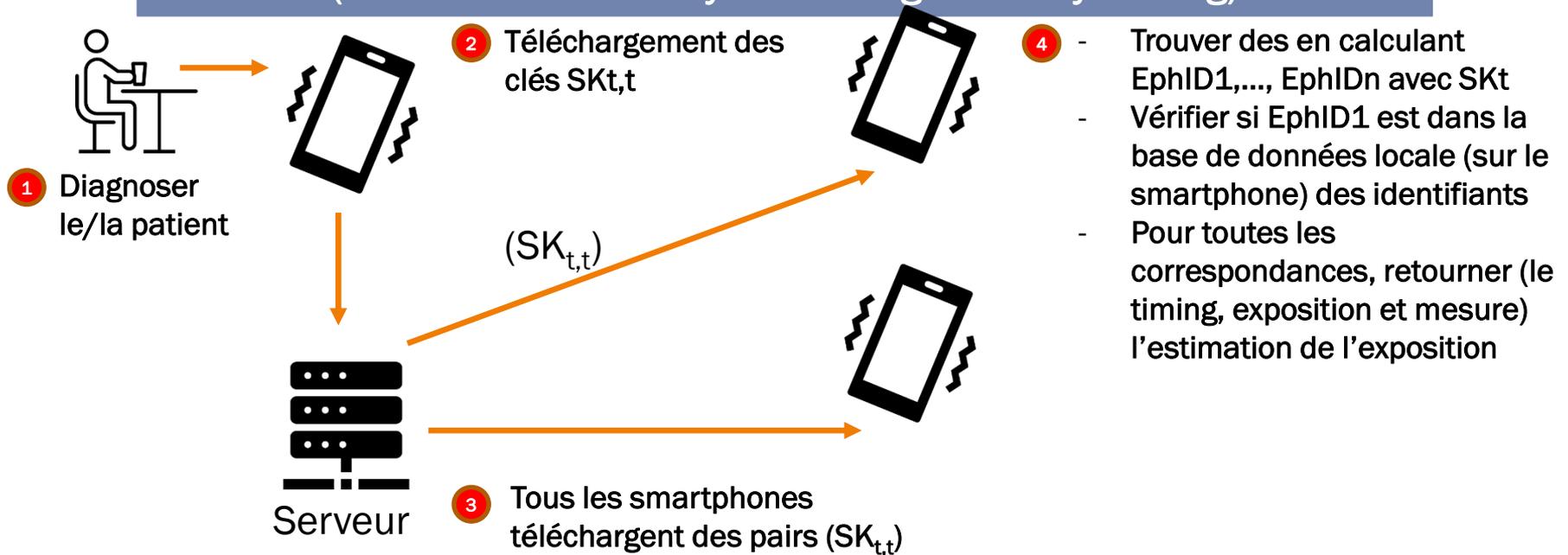
Pour éviter le traçage d'emplacement, chaque EphID a une validité limitée de quelques minutes. Les EphIDs sont reçus par utilisateurs à proximité par des signaux du Bluetooth à basse énergie. Chaque EphID est sauvegardé par ces utilisateurs avec une mesure d'exposition, l'atténuation du signal, et le jour où le radiophare a été reçu. L'application de chaque utilisateur sauvegarde leur propres clés SK_t .





L'APPLICATION COVID AU NIVEAU EUROPÉEN

Le traçage à proximité par DP-3T (Decentralised Privacy-Preserving Proximity Tracing)





L'APPLICATION COVID AU NIVEAU EUROPÉEN

Traitement et stockage des identifiants par Google-Apple API
(Hybrid Decentralised Proximity Tracing)

Bluetooth à basse énergie



Émission RPIs

(Rolling Proximity Identifiers – pseudorandom identifiants émis sur Bluetooth à basse énergie)



Clé d'exposition

temporaire (Temporary Exposure Key) – rafraîchi chaque jour et utilisé pour produire des RPIs en utilisant une fonction de dièse et l'algorithme AES





COMPARAISON DES DIFFÉRENTS ÉTATS MEMBRES

Pays	Autriche	Bulgarie	Croatie
Application centralisé /decentralisé/API Google Apple (G/A)	decentralisé (G/A)	centralisé (propriétaire)	decentralisé (G/A)
Consentement d'utilisateur requis	Consentement éclairé	Consentement éclairé	Consentement éclairé
Politique protégeant la vie privée /détails sur la conformité avec le RGPD	oui		oui
Code source / Localisation du stockage des données	Github /en Autriche et sur Microsoft Azure cloud service	Github/ en Bulgarie	Github / en Croatie

Source: *Demystifying Covid-19 Digital Contact Tracing : A Survey on Frameworks and Mobile Apps*





COMPARAISON DES DIFFÉRENTS ÉTATS MEMBRES

Pays	Chypre	Rép. tchèque	Danemark
Application centralisé /decentralisé/API Google Apple (G/A)	centralisé (propriétaire) GPS,IP, Bluetooth, adresses IP, antenne-relais	v2 decentralisé (G/A) centralisé (propriétaire), BLE (Bluetooth à basse énergie)	decentralisé (G/A)
Consentement d'utilisateur requis	Consentement éclairé	Consentement éclairé	Consentement éclairé
Politique protégeant la vie privée /conformité avec le RGPD	Politique protégeant la vie privée	oui	Politique protégeant la vie privée
Code source / Localisation du stockage des données	/EU	Github/serveurs dans le UE et US	/au maximum 14 jours sur le serveur

Source: *Demystifying Covid-19 Digital Contact Tracing : A Survey on Frameworks and Mobile Apps*





COMPARAISON DES DIFFÉRENTS ÉTATS MEMBRES

Pays	Estonie	Finlande	France
Application centralisé /decentralisé/API Google Apple (G/A)	decentralisé (G/A), BLE	decentralisé (G/A), BLE	v.1 Centralisé, ROBERT, BLE, ultrason
Consentement d'utilisateur requis			
Politique protégeant la vie privée /conformité avec le RGPD	Politique protégeant la vie privée		
Code source / Localisation du stockage des données	Gitlab/ en Estonie (cloud server étatique)	Gitlab / jusqu'à 31.3.21 sur le serveur en Finlande	v. 1 Gitlab/ cloud serveur en France (Outscale)

Source: *Demystifying Covid-19 Digital Contact Tracing : A Survey on Frameworks and Mobile Apps*





COMPARAISON DES DIFFÉRENTS ÉTATS MEMBRES

Pays	Allemagne	Hongrie	Irlande
Application centralisé /decentralisé/API Google Apple (G/A)	decentralisé (G/A), BLE	centralisé (propriétaire), BLE	decentralisé (G/A), BLE
Consentement d'utilisateur requis		Consentement éclairé	Consentement éclairé
Politique protégeant la vie privée /conformité avec le RGPD	oui	Politique protégeant la vie privée	Politique protégeant la vie privée
Code source / Localisation du stockage des données	Github/ au maximum 21 jours sur le serveur	/serveur gouvernemental en Hongrie	Github/cloud server (Amazon Cloud Services)

Source: *Demystifying Covid-19 Digital Contact Tracing : A Survey on Frameworks and Mobile Apps*





COMPARAISON DES DIFFÉRENTS ÉTATS MEMBRES

Pays	Italie	Lettonie	Pays-Bas
Application centralisé /decentralisé/API Google Apple (G/A)	decentralisé (G/A), BLE	decentralisé (G/A), BLE	decentralisé (G/A), BLE
Consentement d'utilisateur requis			Consentement éclairé
Politique protégeant la vie privée /conformité avec le RGPD		oui	Politique protégeant la vie privée
Code source / Stockage des données	Github/ serveur en Italie	sur Github prochainement/ serveur étatique en Lettonie	Github / serveur étatique dans les Pays Bas.

Source: *Demystifying Covid-19 Digital Contact Tracing : A Survey on Frameworks and Mobile Apps*





COMPARAISON DES DIFFÉRENTS ÉTATS MEMBRES

Pays	Norvège	Pologne	Portugal
Application centralisé /decentralisé/API Google Apple (G/A)	centralisé (propriétaire), Bluetooth, GPS	decentralisé (G/A), Bluetooth	decentralisé (G/A), BLE
Consentement d'utilisateur requis			
Politique protégeant la vie privée /politique sur la conformité avec le RGPD		Détails sur les audits en sécurité et la vie privée sont disponibles sur la site web	Politique protégeant la vie privée
Code source / Stockage des données	Déactivé depuis le 16 juin / les données à caractère personnel sur le serveur central seront supprimées	Github / serveur étatique en Pologne	Github /au maximum 14 jours sur le serveur pour l'application

Source: *Demystifying Covid-19 Digital Contact Tracing : A Survey on Frameworks and Mobile Apps*





COMPARAISON DES DIFFÉRENTS ÉTATS MEMBRES

Pays	Slovaquie	Slovénie
Application centralisé /decentralisé/API Google Apple (G/A)	centralisé (propriétaire), BLE, GPS	decentralisé (G/A), BLE
Consentement d'utilisateur requis	Consentement éclairé	Consentement éclairé
Politique protégeant la vie privée /conformité avec le RGPD	oui	oui
Code source / Stockage des données	Github / pour la durée de la période de crise; au maximum 180 jours pour les numéros des smartphone. Les données sont sauvegardées sur les smartphones	Github / Serveur en Slovénie

Source: *Demystifying Covid-19 Digital Contact Tracing : A Survey on Frameworks and Mobile Apps*





COMPARAISON DES DIFFÉRENTS ÉTATS MEMBRES

Pays	Espagne	Suisse
Application centralisé /decentralisé/API Google Apple (G/A)	decentralisé (G/A), BLE	decentralisé (G/A), BLE
Consentement d'utilisateur requis		Consentement éclairé
Politique protégeant la vie privée /conformité avec le RGPD	Politique protégeant la vie privée	Politique protégeant la vie privée
Code source / Stockage des données	Github	Github

Source: *Demystifying Covid-19 Digital Contact Tracing : A Survey on Frameworks and Mobile Apps*



CONCLUSION



RÉFÉRENCES

- BRADFORD, Laura, ABOY, Mateo and LIDDELL, Kathleen. Covid-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes, in *Journal of Law and the Biosciences*, 1-21 doi:10.1093/jlb/ljaa034, Advance Access Publications 28 May 2020
- MARTIN, Tania, KAROPOULOS, Georgios, HERNÁNDEZ-RAMOS, José L., GEORGIOS Kembourakis, and FOVINO, Igor Nai. Demystifying Covid-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps. European Commission, Joint Research Centre, Ispra, Italy. arXiv:2007.11687v2 [cs.CR], 17 September 2020
- LESLIE, Mitch. Covid 19 Fight Enlists Digital Technology: Contact Tracing Apps in *Engineering* (Beijing, China) 16 September 2020. Web. <https://doi.org/10.1016/j.eng.2020.09.001>
- RIZZO, E. COVID-19 Contact Tracing Apps: The 'elderly Paradox' in *Public Health* 185 (2020), 127. <https://doi:10.1016/j.puhe.2020.06.045>





RÉFÉRENCES

- SCANTAMBURLO, Teresa, CORTÉS, Atia, DEWITTE, Pierre, VAN DER EYCKEN, Daphné, BILLA, Valentina, DUYSBURGH, Pieter et LAENENS, Willemien. Covid-19 and Contact Tracing Apps: A Review under the European Legal Framework, arXiv:2004.14665v2 [cs.CY], 18 mai 2020
- SHARMA, Shavneet, SINGH, Gurmeet, SHARMA, Rashmini, JONES, Paul, KRAUS, Sascha, et DWIVEDI, Yogesh K. Digital Health Innovation: Exploring Adoption of COVID-19 Digital Contact Tracing Apps in *IEEE Transactions on Engineering Management* (2020), 1-17.
- MORLEY, Jessica, COWLS, Josh, TADDEO, Mariarosaria et FLORIDI, Luciano. Ethical Guidelines for COVID-19 Tracing Apps in *Nature* 582.7810 (2020): 29-31.
- CIOFFI, A., LUGI, C et Cecanneccchia, C. Apps for COVID-19 Contact-tracing: Too Many Questions and Few Answers in *Ethics, Medicine, and Public Health* 15 (2020): 100575.



MERCI POUR VOTRE ATTENTION!

Association à but non lucratif créée par et pour les professionnels
de la protection des données au Luxembourg



Rejoignez-nous sur www.apdl.lu