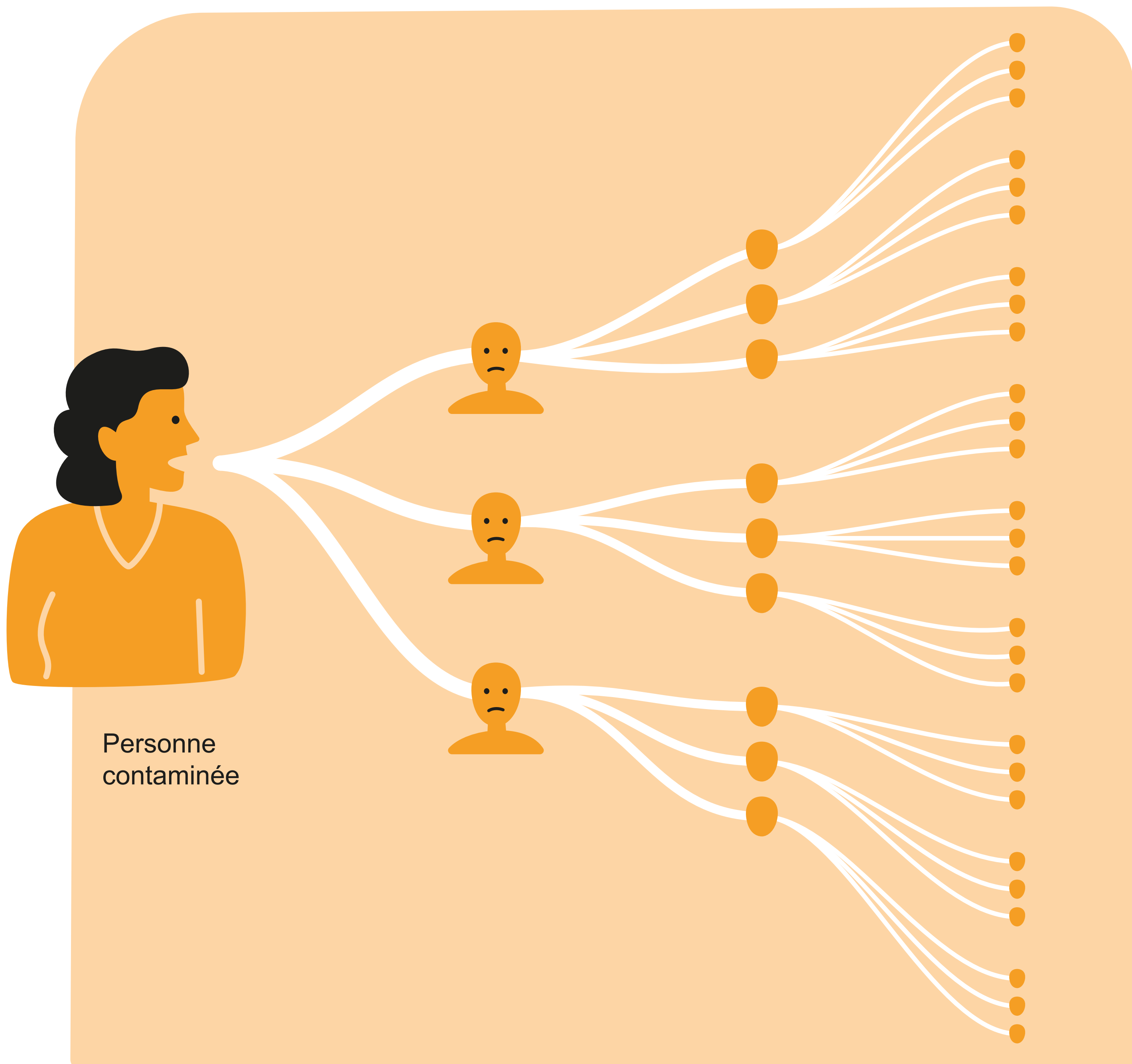


# Protocole ROBERT

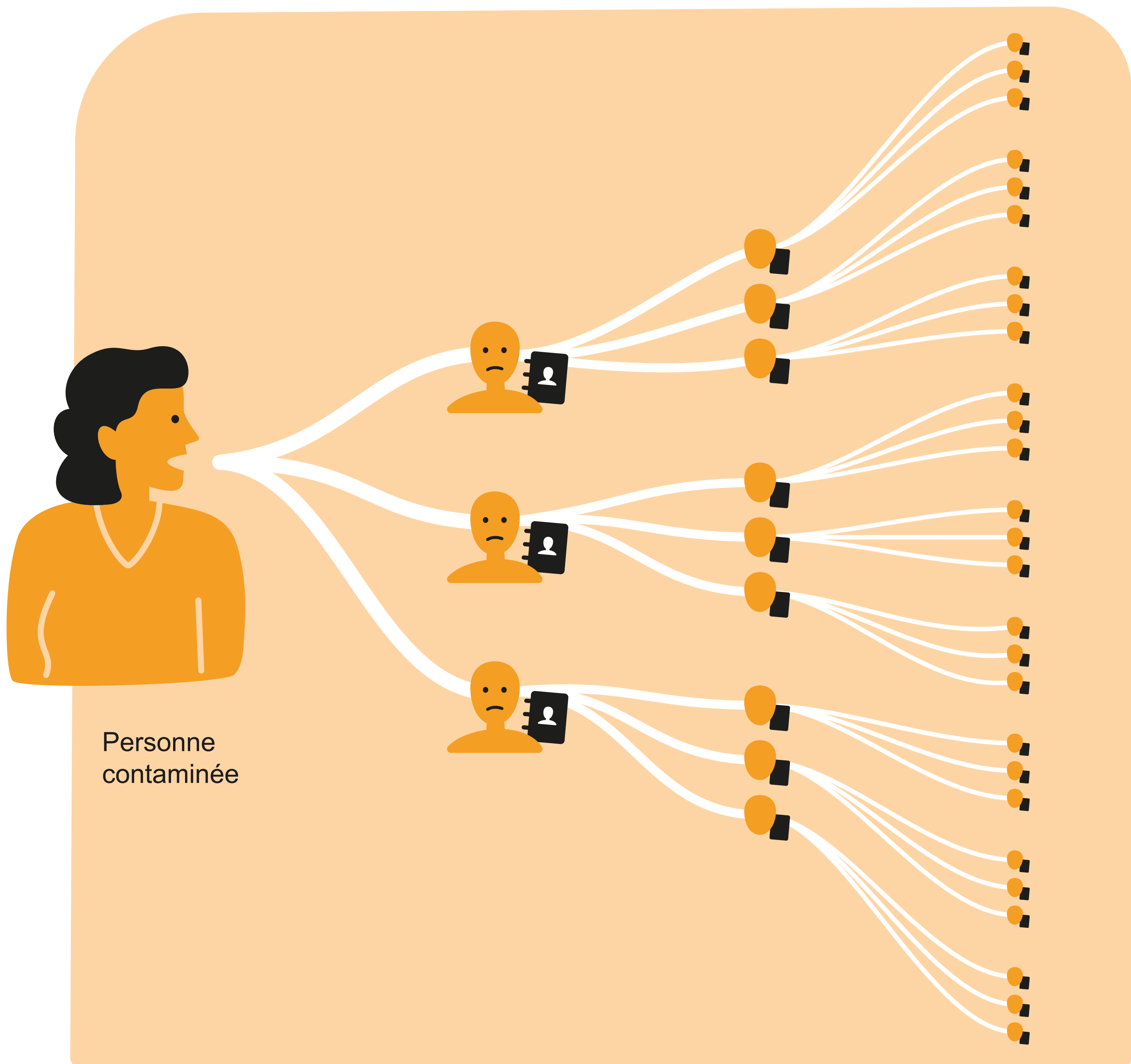
---

**Un protocole de suivi  
des contacts rapprochés,  
rigoureux et respectueux  
de la vie privée.**





Pourquoi le virus Covid19 se répand-il si vite ? Parce qu'une personne peut être contagieuse pendant plusieurs jours sans le savoir et sans présenter de symptômes. Elle peut ainsi transmettre le virus à de nombreuses autres personnes.



Le procédé de traçage traditionnel repose sur des entretiens avec les personnes porteuses du virus. Ce procédé implique la collecte et le traitement des données personnelles de ces personnes infectées (données de géolocalisation notamment) et de celles qu'elles ont rencontrées.



Il est possible de mémoriser l'historique de contacts d'une personne à l'aide d'une application sur téléphone mobile, et de respecter la vie privée, en utilisant simplement les signaux Bluetooth. Nous proposons qu'une telle application soit mise en œuvre en utilisant le protocole ROBERT.



Alice



Bernard



Charles

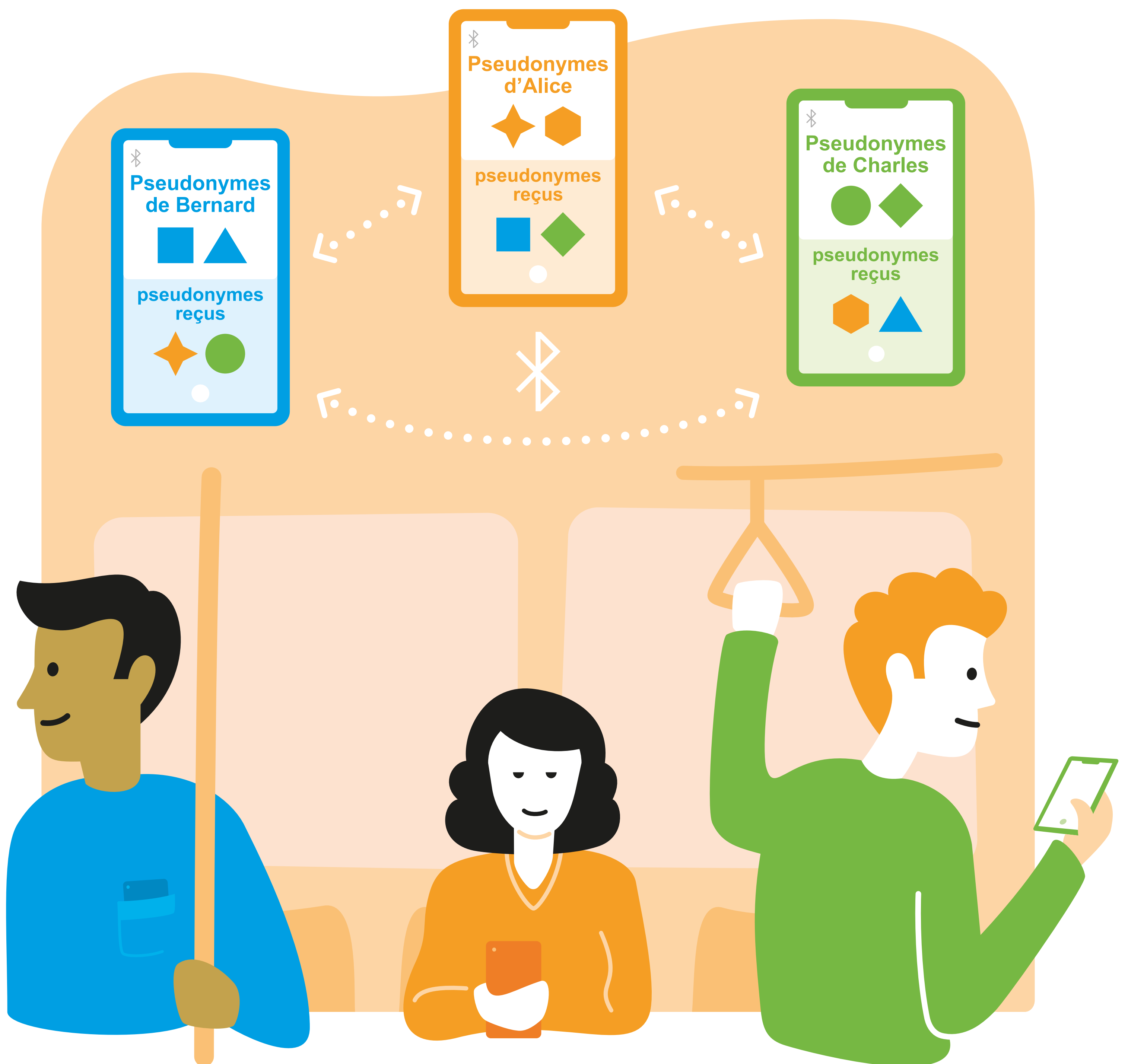
Comment une application peut-elle mémoriser cet historique de contacts tout en protégeant la vie privée de ses utilisateurs ? Suivez l'histoire d'Alice, Bernard et Charles et vous verrez comment fonctionne le protocole ROBERT.



Alice décide d'installer une application basée sur le protocole ROBERT et active la fonction Bluetooth de son téléphone mobile.



Lors de l'installation, une application reçoit plusieurs pseudonymes. Ces pseudonymes seront utilisés les uns après les autres et pour une période limitée, ce qui permet de s'assurer qu'ils ne pourront pas être utilisés pour suivre Alice.



L'application d'Alice envoie ses pseudonymes via le Bluetooth. Seules les applications des personnes entourant Alice, comme Bernard et Charles, sont capables de collecter son pseudonyme et de le stocker sur leurs téléphones.

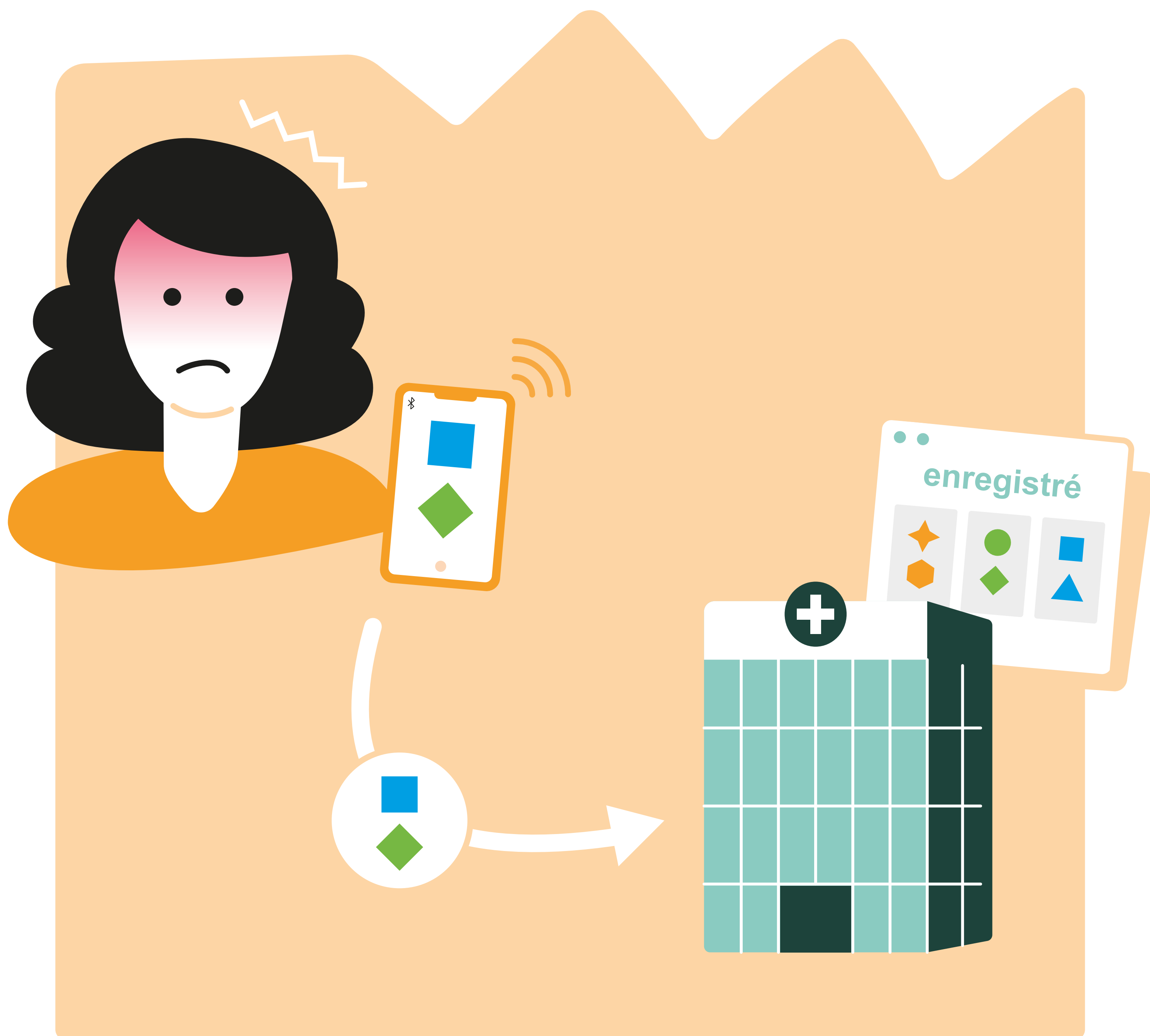




Les pseudonymes des utilisateurs proches d'Alice sont détectés sans utiliser la géolocalisation, grâce à la seule utilisation des signaux Bluetooth, ainsi personne ne saura plus tard où se trouvait Alice.



Quelques jours plus tard, Alice présente les symptômes du Covid19 et se fait tester. Il s'avère qu'Alice a été contaminée depuis un certain temps déjà.



Pour aider à protéger les personnes qu'elle a pu rencontrer au cours des deux dernières semaines, Alice accepte de partager leurs pseudonymes avec la base de données centrale.



L'application de Charles envoie son pseudonyme à la base de données centrale plusieurs fois par jour. Charles reçoit une alerte sur son téléphone portable : au cours des 2 dernières semaines, il a été en contact avec une personne contaminée par le Covid19 ! Bernard reçoit la même alerte sur son téléphone portable.

## FAQ

# UNE APPLICATION REPOSANT SUR LE PROTOCOLE ROBERT POURRAIT-ELLE PERMETTRE DE ME TRACER ?



Non. Prenons l'exemple d'Alice : lors de l'installation d'une application, la base de données centrale envoie plusieurs pseudonymes qui sont associés à son application. Mais la base de données centrale ne sait pas qu'il s'agit d'Alice – elle n'a pas accès à son vrai nom, à son numéro de téléphone ou à sa localisation.

## FAQ

C'EST PAS MAL, MAIS... CHARLES PEUT-IL SAVOIR QUE C'EST ALICE QUI A PU LUI TRANSMETTRE LE VIRUS ?



Non, Charles ne peut pas savoir avec certitude que c'est Alice qui a été diagnostiquée positive au COVID-19. Charles a rencontré beaucoup de personnes pendant les dernières semaines (période de contagiosité) et il n'est pas en mesure de dire qui l'a peut-être infecté.

## FAQ

QUELQU'UN D'AUTRE QUE SON MÉDECIN PEUT-IL APPRENDRE QU'ALICE A ÉTÉ INFECTÉE ?



Non. Le protocole ROBERT garantit que personne, à l'exception du médecin, n'a accès à cette information. Même la base de données centrale n'a pas l'information sur qui a été diagnostiqué positif au COVID-19. La base de données centrale ne reçoit que les pseudonymes temporaires de toutes les personnes qui ont été en contact avec une personne infectée. Dans notre exemple, la base de données centrale ne reçoit que les pseudonymes de Bernard et Charles, mais ne contient aucune information sur Alice.

## FAQ

COMMENT CELA SE PASSE-T-IL POUR ELISA, LA FILLE D'ALICE, QUI N'A PAS DE TÉLÉPHONE MOBILE ?



En effet, les enfants et les personnes qui n'ont pas de téléphone portable ne peuvent pas bénéficier d'une application de ce type. Les chercheurs s'efforcent aujourd'hui de faire en sorte que le protocole ROBERT puisse fonctionner sur un appareil différent qui offre le même service.



## FAQ

### LE PROTOCOLE ROBERT EST-IL UNE APPLICATION POUR TÉLÉPHONE MOBILE ?



Non, le protocole ROBERT n'est pas une application. C'est un protocole de communication – en informatique, cela signifie une "procédure" qui décrit comment une application doit fonctionner. Il est proposé par des scientifiques, qui travaillent sur la sécurité et la confidentialité des protocoles de communication depuis plus de 20 ans. Tout type d'application peut utiliser le protocole ROBERT. Le protocole ROBERT est une proposition qui fait suite à une initiative paneuropéenne de suivi des contacts de proximité préservant la vie privée (PEPP-PT). Son but principal est de garantir le respect des normes européennes en matière de protection des données, de vie privée et de sécurité.

Ce document est en phase avec les spécifications techniques du protocole ROBERT, version 1.0:  
**<https://github.com/ROBERT-proximity-tracing>**

Inria, France<sup>1</sup>  
Fraunhofer AISEC, Allemagne

Avril 2020

—

1. Travail collaboratif d'Inria conduit par l'équipe PRIVATICS.