Protéger des vies ET la liberté

Nous reprenons ici le billet de blog du Framablog “Une appli de traçage du COVID 19 qui échappe à Big Brother ?” que vous pouvez retrouver à l'adresse : https://framablog.org/2020/04/12/une-appli-de-tracage-du-covid-9-qui-echappe-a-big-brother/.

Une appli de traçage du COVID 19 qui échappe à Big Brother ? Ou plutôt pas de traçage du tout ? Oui bien sûr, ce serait sans doute la meilleure solution compte tenu des inévitables “glissements” que redoute comme nous Hubert Guillaud dans cet article.

Mais à l’heure même où se profile l’appli gouvernementale (en France), véritable agneau innocent qui sera inévitablement converti un jour prochain en outil d’espionnage pur et simple, voici une proposition alternative de protocole qui permettrait de freiner la diffusion de la pandémie et d’échapper à la surveillance invasive.

Voici pour comprendre le principe de cette application une bande dessinée, qui est l’œuvre de **Nicky Case** (son site – son patreon), elle est destinée à expliquer le fonctionnement du protocole DP-3T à un public plus large. Elle n’est pas une représentation exacte du protocole, comme elle le précise :

> *Cette BD présente des aspects qui vont au-delà des spécifications de notre protocole, tels qu’un score de risque lié à une instruction de rester à la maison, un exemple ludique de ce à quoi pourrait ressembler un algorithme de calcul de risque local.*
>
> *Bien que notre protocole soit conçu pour protéger la vie privée et pour contribuer à protéger un large éventail de libertés contre les détournements de fonction,* ***il nécessite un déploiement réfléchi dans un environnement avec des politiques informées et protectrices des droits de l’homme afin de fonctionner pour tous les membres de nos communautés.***
>
> ***La bande dessinée ne doit donc pas être lue comme fournissant des suggestions de politiques au-delà du protocole de l’équipe DP-3T.***

Pour celles et ceux qui veulent aller plus loin, beaucoup de précisions sur son fonctionnement, ses limites et ses conditions sont dans cette étude proposée par un pool de scientifiques dont la lecture demande un certain bagage technique (copie locale du document).

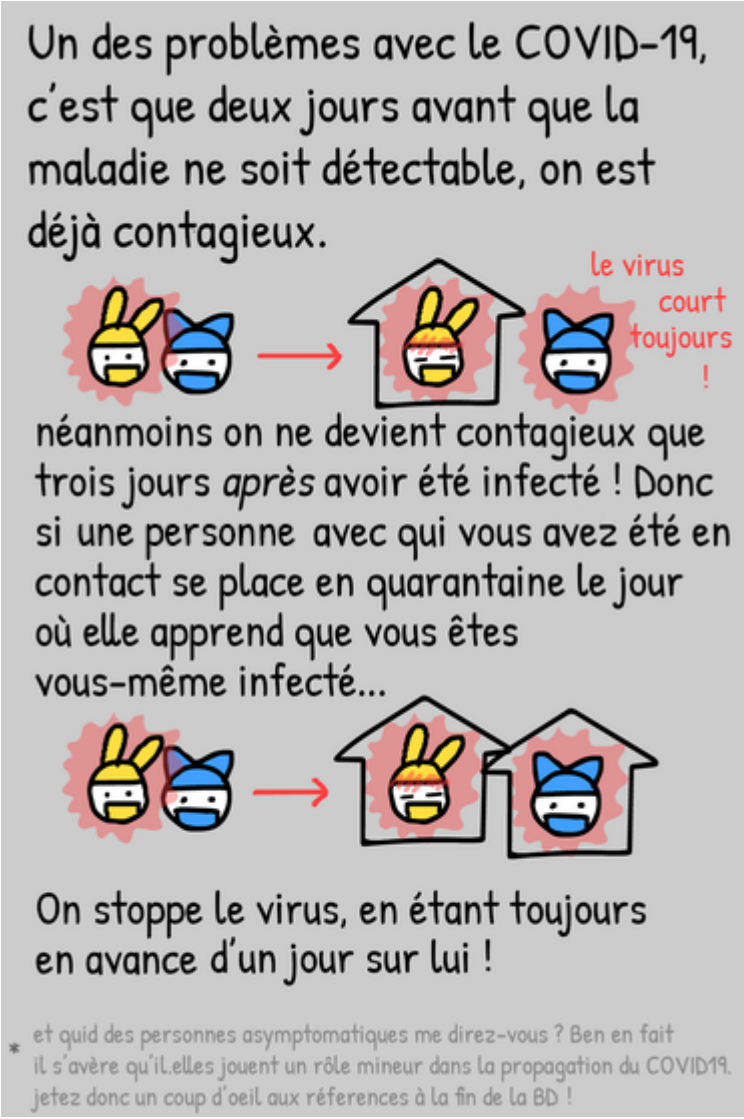
La présente publication ne signifie pas que Framasoft (ainsi que nous logiciel-libre.ch) promeut une quelconque application ni ne la présente comme une solution miracle. Il s’agit seulement d’éclairer le fonctionnement d’un protocole.

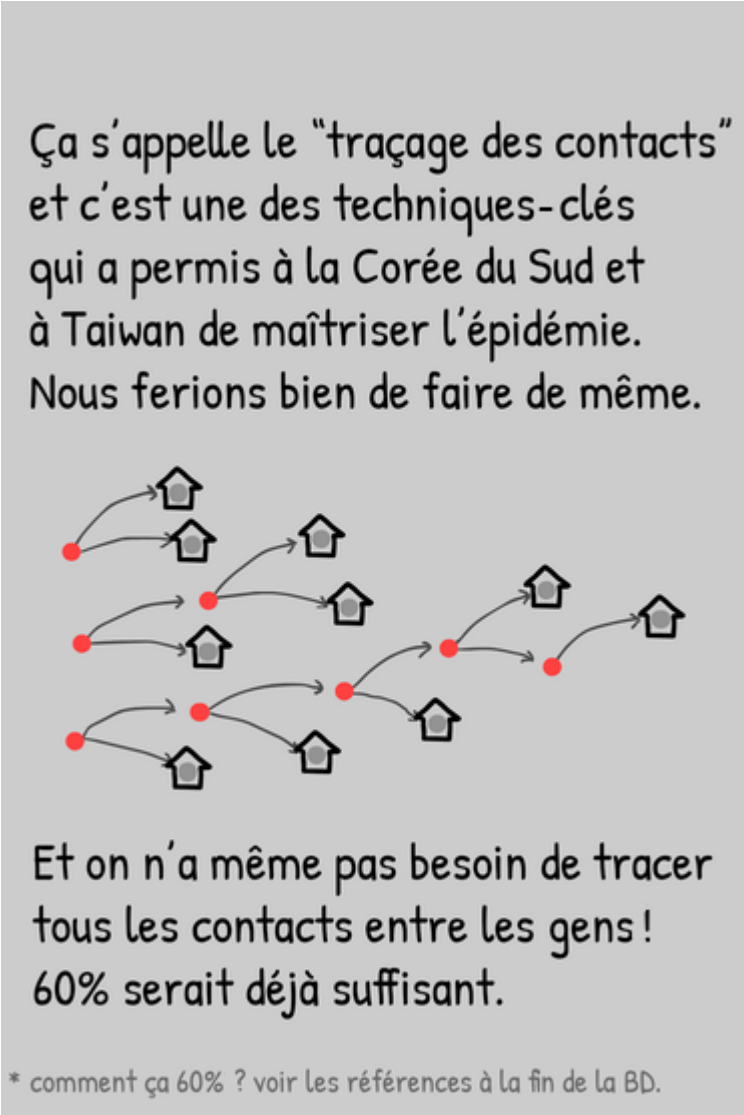
Bande dessinée originale en anglais : https://ncase.me/contact-tracing/

La traduction française que vous pouvez parcourir ci-dessous est due aux efforts conjugués et patients de **Michel “Meï” Mancier** et de **Samuel Hackwill**. Qu’ils en soient vivement remerciés !

La BD en PDF

Protéger des vies et la liberté


Un des problèmes avec le COVID-19, c'est que deux jours avant que la maladie ne soit détectable, on est déjà contagieux.
le virus court toujours !
néanmoins on ne devient contagieux que trois jours *après* avoir été infecté ! Donc si une personne avec qui vous avez été en contact se place en quarantaine le jour où elle apprend que vous êtes vous-même infecté...
On stoppe le virus, en étant toujours en avance d'un jour sur lui !
* et quid des personnes asymptomatiques me direz-vous ? Ben en fait il s'avère qu'il.elles jouent un rôle mineur dans la propagation du COVID19. jetez donc un coup d'oeil aux réferences à la fin de la BD !


Ça s'appelle le "traçage des contacts" et c'est une des techniques-clés qui a permis à la Corée du Sud et à Taiwan de maîtriser l'épidémie. Nous ferions bien de faire de même.
Et on n'a même pas besoin de tracer tous les contacts entre les gens ! 60% serait déjà suffisant.
* comment ça 60% ? voir les références à la fin de la BD.

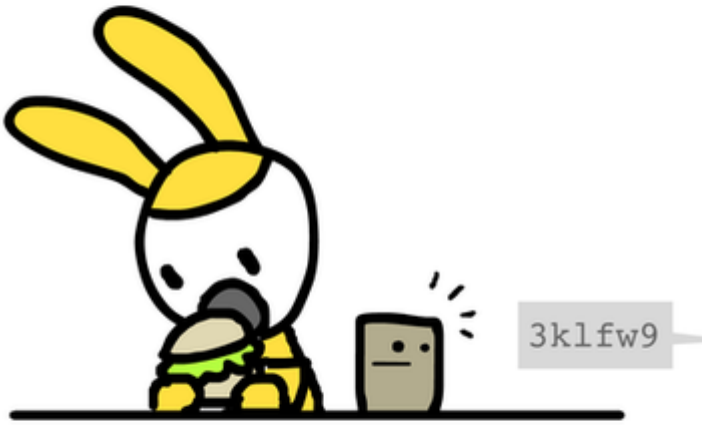
Néanmoins, ce traçage doit quasiment être fait en temps réel pour être efficace. La méthode traditionnelle pour obtenir ces informations (par interrogatoire) est trop lente.
C'est là où les applications de traçage entrent en jeu !
Devrons-nous sacrifier notre vie privée pour autant ?

OH QUE
NON

Il est tout à fait possible de sauver des vies *tout en protégant nos libertés*, à l'aide d'un procédé simplissime !
pour nous l'expliquer voici Alice & Bob ...

Alice télécharge une application de traçage (dont le code est public , ce qui fait qu'on peut vérifier que l'application fonctionne bien comme ceci :)
5lPomk
8jUIL4
l1wda6
toutes les 5 minutes, son téléphone envoie un charabia aléatoire et unique à tous les autres téléphones à proximité, par Bluetooth.
* 5 minutes plus ou moins, c'est un exemple ! par ailleurs techniquement ce sont des messages peudo-aléatoires mais ça ne change rien à notre affaire.

Dans la mesure où les messages sont aléatoires et ne contiennent aucune donnée de géolocalisation, ils ne contiennent AUCUNE information sur l'identité d'Alice ni sur les endroits où elle est allée.



En plus d'envoyer ses messages aléatoires, le téléphone d'Alice reçoit également les messages des autres téléphones à proximité.

Par exemple, celui de Bob.

Bob a installé la même application de traçage sur son téléphone (ou une autre application de traçage respectueuse de sa vie privée et compatible avec celle d'Alice).

Si Bob et Alice restent à proximité plus de 5 minutes, leurs téléphones vont échanger un message aléatoire et unique.

Leurs téléphones se souviennent de tous les messages dits et entendus ces derniers 14 jours.
CE QUE J'AI DIT
aSt5yv l1wda6
8jUIL4 5lPomk
rtxnbk 33trGb
49djv7 ryteq8
12poLV VB490s
CE QUE J'AI ENTENDU
89ckxj 3klfw9
g83kxS wWjcd6
l789xI 439Hxs
59f7y5 zpw7UU
FFyc67 xlc902
Rappel: les messages aléatoires ne contiennent AUCUNE INFO, l'intimité d'Alice est protégée de Bob, et vice versa!
* 14 jours est aussi juste un exemple! les épidémiologistes pourraient apprendre que la "période infectieuse" est en fait plus courte ou plus longue que cela.

Le lendemain, Alice développe une toux sèche et de la fièvre.
Alice se fait tester.
Alice a le COVID-19.
Ce n'est pas un bon jour pour Alice.

Mais elle peut maintenant se venger du virus ! Alice envoie la liste des messages qu'elle a envoyés ces 14 derniers jours à un hopital, en utilisant un code qui lui a été fourni à cet effet par son médecin (c'est pour éviter le spam).

Alice peut également cacher les messages qu'elle veut garder pour elle, comme ceux que l'application a envoyés quand elle était à la maison.

L'Hôpital range les messages aléatoires d'Alice dans sa base de données.
TOUT CE QUE LES COVID19 ONT DIT :
J'insiste encore : ces messages ne contiennent aucune information sur les endroits où elle est allée, sur son identité, *ni même sur le nombre de personnes avec qui elle a été en contact* ! Ces informations ne sont d'aucun usage à l'hôpital.
* Différents hôpitaux peuvent mettre ces bases de données en commun, mais dans la mesure où aucune information personnelle n'y est stockée ça ne présente pas de danger.

...mais pas pour Bob !
CE QUE LES CAS DE COVID-19 ONT DIT
CE QUE J'AI ENTENDU
Le téléphone de Bob vérifie régulièrement la liste de messages de cas du COVID-19 de l'hôpital, et voit s'il a "entendu" n'importe lequel de téléphones proches ces derniers 14 jours.
(Le charabia ne donne à Bob AUCUNE AUTRE INFO PERSONNELLE.)
* le vrai protocole DP-3T est encore PLUS sécurisé ! il utilise une méthode appelée "cuckoo filter" pour que les téléphones ne connaissent QUE les messages covid-19 qu'ils ont entendus, sans révéler TOUS les messages covid-19.

S'il a reçu, mettons, 6 messages envoyés par le téléphone de personnes atteintes de COVID19 (6 * 5 minutes : 30 minutes d'exposition au virus), le téléphone va suggérer à Bob de se placer en quarantaine.

Et ainsi Bob stoppe la propagation du virus, en étant un jour en avance sur lui !

* à nouveau, ces nombres ne sont que des exemples !

Et voilà !

C'est comme ça que le traçage numérique des contacts peut proactivement prévenir la transmission du COVID-19 *tout en* protégeant nos droits.

Merci, Alice & Bob !
Prenez soin de vous.

RÉFÉRENCES :

Cette BD vise à vulgariser le protocole **DP-3T**, tel qu'il fonctionnait en date du 9 avril 2020. En réalité, c'est un truc assez complexe et *très* sécurisé ! pour en savoir plus :

github.com/DP-3T/documents

Il existe un autre protocole similaire, garantissant également la protection de la vie privée, le protocole **TCN** :

github.com/TCNCoalition/TCN

Enfin, vous trouverez ici l'étude de l'université d'Oxford qui montre que les applications de traçage pourraient à elles seules permettre de contenir l'épidémie (*sans* quarantaine généralisée).

Ferretti & Wymant et al. "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing." *Science* (2020).

From:
https://www.logicielslibres.ch/ - **Logiciel libre**

Permanent link:
https://www.logicielslibres.ch/articles/proteger_des_vies_et_la_liberte/accueil?rev=1586788618

Last update: **13.04.2020 @ 16:36**