



David Cormand
Député européen
co-président de la délégation Europe Ecologie
groupe Verts-ALE

Mesdames les Députées,
Messieurs les Députés,
Mesdames les Sénatrices,
Messieurs les Sénateurs,

Paris, le 22 avril 2020

Mesdames et Messieurs les Parlementaires,

Je vous écris au sujet des annonces de déploiement d'une application de « *contact tracing* » Stop Covid. Cette question sera portée à votre attention les 28 et 29 avril prochains. Je tenais à vous alerter sur les risques que nous font courir le dispositif envisagé.

Parfois, le mal se présente à nous paré des atours de la vertu. C'est aujourd'hui le cas. Sous couvert de préoccupations sanitaires que nous partageons toutes et tous, c'est une partie de nos droits fondamentaux que l'on obère, en cédant aux sirènes de la techno-surveillance.

Voilà pourquoi il faut se féliciter que le débat sans vote initialement prévu ait fait long feu. Désormais, grâce à la vigilance commune de l'ensemble des familles de l'opposition, et à des voix qui se sont élevées au sein même de la majorité pour pointer un dysfonctionnement démocratique, vous aurez en conscience à vous prononcer au nom du peuple français. Vous le ferez, sur une application qui n'est pas anodine, mais est porteuse de rupture avec la manière dont nous concevons nos libertés.

Pour ma part, je refuse que la légitime lutte contre la pandémie soit le cheval de Troie de la société de surveillance généralisée.

D'emblée, le débat a été mal engagé. En faisant porter les échanges sur les modalités techniques de l'application, sans que son opportunité et son utilité ne soient vraiment questionnées, il nous a été proposé de foncer tête baissée vers l'inconnu. Remettre le débat sur ses pieds, c'est tenter d'éclairer nos concitoyennes et nos concitoyens sur ce qui est en jeu, et permettre à la société d'avoir un véritable débat sur la question, pour que chacune et chacun, puisse se forger son opinion en son âme et conscience.

Parlons clair. Le déploiement généralisé d'une application de « *contact tracing* » pour lutter contre l'épidémie de coronavirus est-il souhaitable ? Notre réponse est non.

Nous présentons les arguments qui fondent notre refus d'une telle perspective.



David Cormand
Député européen
co-président de la délégation Europe Ecologie
groupe Verts-ALE

1) Surveiller n'est pas prendre soin

Cela laisse penser que la technologie de surveillance numérique est la solution la plus à même pour pallier les manquements et les impréparations des gouvernements successifs – en l'occurrence dans le secteur de la santé.

Si nous devons accepter l'application proposée, cela avaliserait l'idée démocratiquement dangereuse qu'il est acceptable de suivre nos citoyens à la trace au nom d'un intérêt général supérieur. Funeste précédent dont on voit mal ce qui éviterait qu'on y fasse référence demain pour justifier qu'on recourt au même procédé pour d'autres motifs, mais bientôt pour notre « sécurité », pour la croissance, ou pour la raison d'État.

2) Il n'est pas possible de garantir l'anonymat des données conservées

Tout protocole de traçage nécessite de constituer un fichier des personnes croisées, que la solution soit décentralisée ou non. Ce fichier de donnée est pseudonymisé, mais il est possible de retrouver l'identité des personnes en les combinant à d'autres informations de la base de données ou hors de cette base de données, comme l'ont prouvé des recherches sur la question.

Les experts en cybersécurité nous alertent sur les failles de sécurité associées à l'activation continue du Bluetooth, et recommandent de le désactiver aussi souvent que possible. Chaque appareil connecté en Bluetooth pouvant détecter et enregistrer les appareils à proximité, cela crée un risque d'appropriation des données et de ré-identification des malades.

3) Nous nous dirigeons vers le mauvais choix d'un système centralisé

Une lettre ouverte de trois cents chercheuses et chercheurs à travers le monde publiée ce lundi 20 avril rappelle avec insistance qu'une application respectueuse de la vie privée des utilisateurs devrait impérativement utiliser une infrastructure décentralisée. Le Parlement européen a adopté sans équivoque la condition d'une infrastructure décentralisée dans sa résolution de réponse à l'épidémie adoptée le vendredi 18 avril.

Le projet européen PEPP-PT, actuellement soutenu par le gouvernement français, ayant finalement choisi une structure centralisée ne nous laisse rien présager de bon sur le résultat à venir.

Dans le cas d'un système centralisé, la base de données serait envoyée à une autorité centrale qui croiserait les données en cas de déclaration d'infection pour prévenir les malades, et pourra donc retrouver l'identité des personnes infectées si elle le souhaite.



David Cormand
Député européen
co-président de la délégation Europe Ecologie
groupe Verts-ALE

4) Le Bluetooth est inefficace, mais sa généralisation dans le quotidien est une menace invisible pour nos libertés

Le choix du Bluetooth génère de grandes limites techniques. Il ne permet ni une estimation précise de la distance entre individus, ni de repérer s'il y a un mur ou un étage entre deux personnes, ou encore si quelqu'un porte correctement un masque. Il n'est donc pas techniquement capable de détecter rigoureusement qui a fait l'objet d'un contact à risque avec une personne infectée.

Ainsi, le système enregistrerait probablement beaucoup trop de contacts : en zone dense, certaines personnes seraient alertées quotidiennement ! Nous risquons assurément d'encombrer les trop faibles capacités de dépistage dont dispose notre pays. À moyen terme le manque de fiabilité mènerait certaines personnes à ne pas donner crédit aux alertes de l'application, neutralisant ses effets.

Par contre, un système fonctionnant au Bluetooth permet *de facto* un traçage généralisé des individus : le signal est facilement détectable, et son activation généralisée serait une aubaine pour les entreprises d'analyse de données qui pourraient les collecter de façon systématique dans l'espace public pour les monnayer. Des chaînes de grands magasins l'utilisent déjà pour tracer les clients qui se promènent en leur sein et mieux cibler la publicité qui leur est dédiée. Qui peut dire quel usage en sera fait demain ?

5) Nous ne devrions habituer personne à renoncer à sa vie privée

Pour être prétendu efficace, il faudrait que 70 % ou plus de la population souscrive et se soumette au dispositif de pistage. Comme le droit du numérique repose sur le principe de consentement, et que celui-ci ne doit être ni imposé par la réglementation, ni par les entreprises, ni par la pression sociale, qu'est-ce qui nous laisse penser que ce seuil de 70 % puisse être atteint ?

La question de la pression sociale n'est pas à négliger. En Corée, il y a des exemples de chasse aux sorcières pour retrouver et dénigrer publiquement les personnes infectées, transformant l'application en un système de dénonciation des malades.

6) L'application proposée légitime de fait la mainmise des GAFAM sur nos données.

En demandant à la population d'accepter son traçage au nom l'argument selon lequel c'est déjà en partie chose faite, nous entérinons la politique du fait accompli sur lequel misent les GAFAM pour asseoir leur empire sur nos vies. Hier, nos données ont été dérobées en douceur. Nous ne savions pas quel monde se préparait par le téléchargement de nos applications. Mais les mauvaises habitudes ne doivent pas faire force de loi. Il faut au



David Cormand
Député européen
co-président de la délégation Europe Ecologie
groupe Verts-ALE

contraire prendre conscience que nos données, aujourd'hui collectées par les GAFAM sans consentement véritablement libre et éclairé, sont précieuses et doivent être protégées.

Google, Apple, ou Facebook ont saisi l'opportunité du coronavirus pour tenter de se légitimer comme acteurs du bien commun. Mais nous avons la mémoire longue. Le scandale Cambridge Analytica a montré que nos démocraties étaient vulnérables face à l'exploitation malveillante de nos informations personnelles. La marchandisation de nos vies a ouvert la voix à une manipulation démocratique de grande ampleur. Nous devons avoir la même vigilance sur l'utilisation faite de nos données par l'État.

7) Si une telle application voit le jour, il n'y aura probablement pas de retour en arrière

À celles et ceux, enfin, qui pensent que c'est un mauvais moment à passer et que nous pouvons suspendre un instant notre vigilance, je veux dire qu'il est illusoire de raisonner ainsi. L'histoire nous a prouvé que nos démocraties ne parviennent pas à rendre les libertés qu'elles suspendent en temps de crise.

L'urgence est mauvaise conseillère qui nous pousse à adopter des mesures sans prendre le temps de soupeser longuement leurs avantages et inconvénients, sans regarder de près leurs limites et leurs risques. Une fois l'urgence passée, nous gravons dans le marbre de l'habitude les enfreintes que nous refusions hier, acceptant les nouvelles limites, les restrictions de libertés, la perpétuation de la surveillance.

Nous nous battons actuellement au Parlement européen pour défendre nos libertés et nos démocraties en bloquant ce type de pratique à l'échelle européenne. Vous pouvez compter sur notre soutien déterminé pour combattre la mise en place d'une société de surveillance généralisée et la confiscation de nos droits numériques.

Le temps court ne doit pas cannibaliser l'avenir. Une civilisation qui abolit le sens de la durée court à sa perte. Je vous conjure donc de résister à la pression de l'instant pour défendre nos libertés séculaires.

Bien respectueusement,

David Cormand,
Député européen