ASSEMBLÉE NATIONALE

15ème législature

Utilisation de la technologie « blockchain » pour « StopCovid »

Question écrite n° 29649

Texte de la question

M. Julien Aubert interroge M. le secrétaire d'État auprès du ministre de l'économie et des finances et du ministre de l'action et des comptes publics, chargé du numérique, sur l'utilisation de la technologie *blockchain* pour le développement de l'application « StopCovid ». En effet cette application, qui devrait reposer sur un système de traçage *via* la connexion *bluetooth*, comporte des risques très importants concernant la protection des données des utilisateurs et de possibles atteintes à leur vie privée. Quand bien même celle-ci reposerait sur le volontariat, les utilisateurs sont en droit de bénéficier d'une protection extrêmement rigoureuse de leurs données personnelles. Pour répondre à cette exigence, des chercheurs mettent en avant la technologie des *blockchain* qui, selon eux, permettrait d'assurer une telle protection. Ils expliquent qu'une application fondée sur une *blockchain* rendrait impossible toute manipulation des données enregistrées, qui constitueraient ainsi une forme de registre sécurisé. Compte tenu des inquiétudes vives et légitimes des Français sur la protection de leurs données, il souhaiterait ainsi savoir si les services travaillant actuellement sur cette application, en particulier les services de l'Agence nationale de la sécurité des systèmes d'information, ont envisagé le déploiement d'une *blockchain*. Plus précisément, il lui demande de lui préciser si ces services considèrent que cette technologie pourrait apporter des garanties suffisantes en matière de protection contre le vol de données.

Texte de la réponse

La mise en place de l'application StopCovid, validée à la fois par l'Assemblée nationale et le Sénat suite à un débat le fondement de l'article 50-1 de la Constitution du 4 octobre 1958, s'inscrit dans une stratégie plus globale de gestion de la crise sanitaire liée au « déconfinement ». Elle s'envisage ainsi comme un outil complémentaire et un geste barrière supplémentaire. Lorsqu'une personne ayant téléchargée l'application aura été à proximité plus de 15 minutes à moins d'un mètre d'une personne s'étant déclarée sur l'application comme ayant étyé testée positive, elle recevra une notification directement sur son smartphone pour lui donner les consignes sanitaires adéquats (soit s'isoler, contacter un médecin et accéder à un test). L'utilité de l'application réside donc à la fois dans le complément apporté aux services de santé pour retracer les personnes ayant été en contact avec des personnes testées positives au covid et dans la rapidité avec laquelle cela se fait – rapidité précieuse pour que ces dernières n'infectent pas d'autres personnes à leur tour. Sur le plan technique, le projet a été conçu pour apporter le plus haut niveau de sécurité possible et se conformer au principe de minimisation des données utilisées. L'utilisation de la technologie Bluetooth permet le meilleur compromis entre efficacité et sécurité. Le protocole de communication ROBERT – pour ROBust and privacy-presERving proximity Tracing – a définit des spécifications techniques de communication par Bluetooth limitant au maximum les informations transmises entre les téléphones disposant de l'applicationce qui limite les risques. De plus, l'utilisation de l'algorithme de chiffrement a été validé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'hébergement a été confiée à Outscale, seul prestataire d'hébergement qualifié SecNumCloud par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). L'ANSSI a enfin lancé un bug bounty à travers toute l'Europe qui a permis de tester la vulnérabilité du système à des attaques et d'apporter les évolutions nécessaires. StopCovid a été conçu pour qu'il soit impossible de reconstituer les interactions sociales

entre les utilisateurs mais aussi la liste des personnes ayant été testées positives. L'application n'exige aucune donnée permettant d'identifier l'utilisateur (nom, adresse, numéro de téléphone portable). Les données échangées sont des pseudonymes. En cas de notification il est impossible de connaitre la personne à l'origine. La durée de conservation des données est limitée au minimum nécessaire, notamment les pseudonymes constituant l'historique de proximité qui sont effacés tous les 14 jours. Le stockage de l'historique de proximité est effectué sur les téléphones tant que la personne n'entre pas de preuve d'un test positif et ne décide volontairement de partager son historique de proximité. Ces principes auraient été difficilement conciliables avec l'utilisation de la blockchain. Pour toutes ces raisons et en prenant en compte les recommandations en matière de sécurité de l'ANSSI, l'application a été développée sans envisager l'utilisation d'une technologie blockchain.

Données clés

Auteur : M. Julien Aubert
Circonscription : Vaucluse (5e circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 29649
Rubrique : Numérique
Ministère interrogé : Numérique
Ministère attributaire : Numérique

Date(s) clée(s)

Question publiée au JO le : 19 mai 2020, page 3467
Réponse publiée au JO le : 30 juin 2020, page 4596