Association for Computing Machinery
acmpo@acm.org | @acmpolicy
www.acm.org/public-policy/europe-tpc

5 mai 2020

DÉCLARATION SUR LES PRINCIPES ET BONNES PRATIQUES ESSENTIELS POUR LES APPLICATIONS DE TRAÇAGE DE CONTACTS COVID-19

L'émergence et la propagation rapides du virus SRAS-CoV-2 et de l'infection COVID-19 ont amené les gouvernements du monde entier à ordonner différents degrés de confinement à une grande partie de la population mondiale. Ces gouvernements envisagent maintenant quand et comment assouplir ou lever ces restrictions sans provoquer d'effet de rebond qui relancerait l'épidémie. En l'absence de remède ou de vaccin, les épidémiologistes recommandent un ensemble de mesures, y compris la distanciation sociale, les tests à grande échelle et le traçage des contacts pour identifier ceux qui ont été en contact avec des personnes infectées.

Diverses applications de traçage de contacts ont été présentées comme un moyen d'automatiser et d'étendre à des populations entières la surveillance normalement effectuée par le biais d'enquêtes humaines. Ces applications reposent sur l'utilisation de la technologie sans fil Bluetooth pour identifier lorsque deux smartphones se trouvent à proximité l'un de l'autre pendant une durée déterminée.[1]

Le Comité européen de politique technologique de l'Association for Computing Machinery (Europe TPC) a pour objet de fournir aux décideurs politiques et au grand public des informations techniques au service de la définition de politiques publiques saines. En ce qui concerne les systèmes de traçage de contacts en cours d'étude, Europe TPC constate que :

- Si tous les protocoles de traçage de contacts actuellement proposés peuvent être affinés sur le plan technologique afin de maximiser la confidentialité et l'anonymat,[2] ces applications restent très vulnérables aux attaques.[3] En conséquence, les ***applications de traçage de contacts connues à l'heure actuelle ne peuvent pas préserver pleinement la vie privée et l'anonymat des personnes ;***

[1] Les téléphones équipés de ces logiciels échangent des identifiants afin de pouvoir conserver une trace des téléphones avec lesquels ils ont été « en contact ». Lorsqu'une personne est identifiée comme ayant été infectée, les téléphones avec lesquels la personne infectée a été en contact sont notifiés afin que leurs propriétaires puissent prendre les mesures appropriées. Le protocole DP-3T adopte une approche dite décentralisée (l'identifiant du « téléphone infecté » est téléchargé sur un serveur central et diffusé à tous les autres téléphones, qui peuvent alors rechercher une correspondance dans leur liste de contacts récents). Le protocole ROBERT utilise une méthode dite centralisée (les téléphones dont les propriétaires sont déclarés infectés téléchargent leurs listes de contacts récents vers un serveur central afin que ces téléphones puissent être notifiés).

[2] Par exemple, des identifiants numériques uniques peuvent être générés de manière aléatoire au lieu d'utiliser les moyens conventionnels d'identification des téléphones ou de leurs propriétaires, et ces identifiants peuvent être changés à intervalles réguliers. Des clés cryptographiques peuvent être utilisées pour sécuriser les transmissions et il n'est pas nécessaire de recueillir des données de géolocalisation. En outre, la collecte de données ou de métadonnées par les autorités centrales des serveurs qui pourraient permettre de reconstituer l'identité d'un téléphone ou d'une personne pourrait être interdite.

[3] Voir, par *exemple*, Analyse de DP3T, Entre Scylla et Charybde, Serge Vaudenay, IACR eprint 2020/399 ou Le traçage anonyme, dangereux oxymore, Xavier Bonnetain et al., risques-tracage.fr.

- ***La fiabilité des applications de traçage de contacts n'est pas prouvée et ne peut être supposée pour de multiples raisons techniques.*** Plus précisément, la technologie Bluetooth n'a pas été conçue pour mesurer les distances entre les appareils ; elle ne peut pas reconnaître quand les appareils connectés sont séparés par un mur ou un flux d'air ; elle peut ne pas enregistrer les appareils à proximité, en fonction de plusieurs facteurs[4]. Le traçage de contacts par Bluetooth semble donc susceptible de surdéclarer des contacts et de générer un grand nombre de faux positifs ;

- ***Une qualité technique élevée et des fonctionnalités avancées ne suffiront pas à elles seules pour que la technologie de traçage de contacts soit efficace***. Plusieurs millions de personnes doivent installer l'application pour que le système enregistre une fraction importante de tous les contacts interpersonnels[5]. La confiance du public dans la protection des données personnelles et de la vie privée est donc une condition préalable essentielle au succès de tout programme de contrôle et de traçage technologique des infections. En conséquence, des mesures légales et/ou réglementaires qui offrent des garanties solides — et qui sont largement comprises par le public — doivent être mises en place.

En tant qu'organisme d'experts techniques, Europe TPC ne prend pas position sur la question de savoir si et quand — du point de vue médical, social, politique et économique — la technologie de traçage de contacts devrait être déployée en Europe compte tenu des réalités technologiques et sociales identifiées ci-dessus. Nous fournissons plutôt des informations techniques pertinentes qui permettront aux décideurs politiques de ***mener des analyses de risques et de coûts-bénéfices minutieuses des conséquences du déploiement à grande échelle d'une technologie non testée dans des circonstances nouvelles avant de prendre de telles décisions***.[6]

Toutefois, si les gouvernements choisissent d'utiliser ces systèmes, nous les invitons à n'utiliser que ceux qui, de par leur conception technique et juridique :

- Respectent et protègent les droits de tous les individus ;
- Protègent les données personnelles et la vie privée au plus haut degré techniquement possible ;
- Sont soumis à l'examen de la communauté scientifique et de la société civile avant, pendant et après le déploiement.

À cette fin, le Comité européen de la politique technologique de l'ACM demande instamment que les principes et bonnes pratiques ci-joints concernant l'architecture, la transparence, la surveillance, les garanties et la participation du public soient rigoureusement appliqués dans le développement et le déploiement de toute technologie de traçage de contacts qui pourrait être utilisée pendant la pandémie COVID-19, dans l'intérêt de l'efficacité technique, de la confiance du public et de la santé publique.

[4] Voir, par exemple, l'analyse du forum GitHub Open Trace Calibration.

[5] Voir, par exemple, Science : La quantification de la transmission du SRAS-CoV-2 suggère un contrôle des épidémies grâce à la recherche numérique des contacts et The Lancet : Faisabilité de la lutte contre les épidémies de COVID-19 par l'isolement des cas et des contacts.

[6] En ce qui concerne l'évaluation des risques, nous avons constaté des vulnérabilités de sécurité inhérentes à la technologie Bluetooth. On peut donc s'attendre à ce que les entreprises criminelles organisées cherchent à tirer profit de l'activation nouvelle et toujours active de Bluetooth sur des millions de téléphones intelligents en Europe. (Cela n'a pas été un problème grave jusqu'à présent car la plupart des gens ne l'utilisent que pour une durée limitée ou dans des situations contrôlées, comme dans leur maison ou leur voiture). En ce qui concerne les coûts, on notera que la Belgique a renoncé pour l'instant à déployer une application de traçage de contacts (voir Lire Coronavirus : la Belgique renonce à une application de traçage des malades) et que la ville de Valence en Espagne expérimente le « traçage basé sur les citoyens » (POLITIQUE - Confidentiel UE, 25 avril 2020).

Europe Technology Policy Committee

Association for Computing Machinery
acmpo@acm.org | @acmpolicy
www.acm.org/public-policy/europe-tpc

PRINCIPES ET BONNES PRATIQUES ESSENTIELS DES APPLICATIONS DE TRAÇAGE DE CONTACTS

Architecture technique

- L'interopérabilité transfrontalière doit être requise pour toute technologie de traçage de contacts afin de faciliter les voyages internationaux et détecter la propagation internationale de l'infection, de nombreux voyageurs qui contractent le virus ne présentant des symptômes qu'à leur retour ;
- Toutes les applications de traçage de contacts, même après leur téléchargement, doivent être conçues de manière à exiger un accord individuel à l'activation de l'application (« opt-in ») et à permettre sa désactivation/réactivation ;
- Une fois activées volontairement, toute application de traçage de contacts doit être conçue de manière à exiger clairement que l'utilisateur consente également à partager des informations personnelles, y compris toute déclaration selon laquelle l'utilisateur a été infecté ou considéré par les autorités comme ayant été exposé à l'infection ;
- Aucune information personnelle sensible, y compris l'état d'infection et d'exposition, ne doit être conservée sur l'appareil d'une personne ou, si elles sont stockées, doivent être protégées par un mot de passe et être cryptées.

Transparence en matière de développement

- Tous les codes sources des applications et des serveurs, et pas seulement les protocoles sous-jacents, doivent être rendus publics ;
- Le code source doit être ouvert à l'examen des experts pendant tout le processus de développement, et pas seulement après qu'un système soit prêt à être déployé ;
- Tous les aspects des processus par lesquels une technologie spécifique de traçage de contacts est sollicitée et obtenue, y compris des données solides concernant tout fournisseur de technologie individuel ou d'entreprise sélectionné, doivent être rapidement rendus publics ;
- Les conflits d'intérêts réels ou perceptibles de toute personne, entité ou consortium développant une technologie de traçage de contacts (ou une technologie adaptable à cette fin) doivent être rapidement mis en évidence et rendus publics.

Surveillance par des experts

- Un comité scientifique indépendant devrait être établi dans chaque pays (ou chaque groupe de pays agissant de concert) où le déploiement de la technologie de traçage de contacts est envisagé, afin d'informer techniquement son développement, de conseiller les décideurs politiques sur ses performances techniques et ses impacts sociaux probables, de fournir des évaluations post-déploiement de l'efficacité de la technologie aux décideurs politiques et au public, et d'offrir des recommandations concernant sa désactivation ;
- Les travaux de tous ces comités devraient être totalement transparents pour le public, enregistrés et conservés de façon permanente, de manière à ce que le public puisse y avoir accès et effectuer des recherches facilement ;

- Ces comités devraient être composés d'experts en :
    - Disciplines techniques (par exemple la cryptographie, les systèmes distribués, la gestion des données, l'interface et l'expérience utilisateur) pour garantir que les meilleurs algorithmes et les meilleures pratiques de leurs domaines sont utilisés dans le développement des systèmes, y compris en particulier les principes de respect de la vie privée dès la conception (« privacy by design ») et de sécurité dès la conception (« sécurity by design »);
    - Sciences sociales pour maximiser l'acceptabilité des applications proposées par la population en général, et l'impact potentiel de ces applications sur les relations sociales, y compris en particulier les risques d'exclusion numérique, de discrimination, de stigmatisation ;
    - Questions juridiques afin d'assurer la conformité aux lois et règlements applicables (par exemple le RGPD).

Garanties juridiques

- Des garanties solides régissant l'utilisation de la technologie de traçage de contacts doivent être adoptées avant le déploiement de cette technologie et être applicables à tous les gouvernements concernés, aux autorités publiques et aux entités privées gérant cette technologie. Ces garanties devraient, au minimum, inclure des exigences, légales ou autres, claires :
    - L'utilisation de l'infrastructure technique n'est autorisée que pour le traçage électronique des contacts liés à la lutte contre la pandémie COVID-19, et toute autre utilisation est explicitement interdite ;
    - Les données recueillies par les applications de traçage de contacts autorisées ne peuvent être conservées que pendant la durée nécessaire au traitement de ces données, et expressément à aucune autre fin ;
    - Aucune personne n'est tenue d'installer, d'activer, d'utiliser, de déclarer ou de révéler le statut d'une application de traçage de contacts ;
    - Aucune personne, entité de quelque nature que ce soit, ou organisme gouvernemental n'est autorisé, sous peine de poursuites judiciaires, à utiliser une technologie conçue pour surveiller l'installation ou l'utilisation d'une application de traçage de contacts ;
    - Les systèmes autorisés de traçage de contacts COVID-19 seront rapidement désactivés lorsque les organismes de santé publique mondiaux parviendront à un consensus sur la fin de la pandémie (par exemple lorsque des thérapies et/ou des vaccins efficaces et fiables seront largement disponibles) ;
    - De tels systèmes doivent également être mis hors service rapidement s'ils sont jugés inefficaces par des organes de contrôle spécialisés (par exemple parce qu'ils sont insuffisamment adoptés, parce qu'ils enregistrent un nombre inacceptable de faux positifs, ou parce qu'ils sont incompatibles en pratique avec les libertés publiques fondamentales).

Engagement du public et de la société civile

- Des mécanismes nationaux et trans-nationaux devraient être utilisés pour solliciter les commentaires du public et des représentants de la société civile sur la technologie de traçage de contacts proposée et sur tous les aspects de son déploiement prévu (en reconnaissant que ces procédures peuvent devoir permettre des actions rapides) ;
- Au minimum, ces processus devraient inviter à formuler des commentaires concernant :
    - Les droits individuels fondamentaux à la vie privée, pierre angulaire des démocraties européennes ;

- La meilleure façon de communiquer au public les informations concernant les applications de traçage de contacts et leur déploiement afin de maximiser leur efficacité en favorisant un sentiment d'objectif commun ;
- Le meilleur moyen d'évaluer et d'atténuer la fracture numérique et les autres effets potentiellement exclusifs ou discriminatoires de cette technologie sur tous les groupes de population, en particulier les plus vulnérables.

5 mai 2020

L'Association for Computing Machinery (ACM) est la plus grande et la plus ancienne société professionnelle au monde regroupant des individus impliqués dans tous les aspects de l'informatique. Son comité européen de politique technologique promeut une politique publique saine et la compréhension par le public d'un large éventail de questions à l'intersection de la technologie et de la politique.

Les auteurs principaux de ce document pour le Comité européen de politique technologique de l'ACM sont Michel Beaudouin-Lafon, Enrico Nardelli et Gerhard Schimpf. Les membres contributeurs sont Panagiota Fatourou, Mario Fritz, Fabrizio Gagliardi, Oliver Grau et Chris Hankin.