Peur du traçage - Traçage de la peur

Jean-Gabriel Ganascia

▶ **To cite this version:**

Jean-Gabriel Ganascia. Peur du traçage - Traçage de la peur. Revue de neuropsychologie, 2021, 13 (2), pp.148-152. 10.1684/nrp.2021.0676 . hal-03287801

HAL Id: hal-03287801
https://hal.science/hal-03287801

Submitted on 15 Jul 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Peur du traçage — traçage de la peur

Fear of tracing — tracing of fear

Jean-Gabriel Ganascia
Professeur Sorbonne Université
Équipe ACASA, LIP6 (UMR 7606 CNRS),
Campus Pierre et Marie Curie
B.C. 169, 4 place Jussieu, 75252, Paris, Cedex 05, France
Jean-Gabriel.Ganascia@lip6.fr

Préambule

Prenant modèle sur les stratégies déployées en Asie du sud-est, beaucoup de pays occidentaux développèrent des outils numériques de traçage en vue de maîtriser la propagation de la CoViD-19 dans la population. Ces dispositifs suscitèrent de multiples craintes dans l'opinion publique. Beaucoup y virent une atteinte irrémédiable aux droits fondamentaux, en particulier aux libertés d'aller et venir, de pensée, de conscience, de religion et de réunion. Cet article tente d'examiner les fondements de ces peurs et de les mettre en regard tant des dangers encourus que des bénéfices espérés, puis de montrer comment ces peurs semblent s'être évanouies soudain, sans raison.

Traçage

Traçage vient de tracer, suivre à la trace, repérer et agréger les indices d'une présence ou d'une activité. Les dispositifs numériques — téléphones portables, objets connectés, caméras de surveillance, navigateurs, ordinateurs personnels etc. — enregistrent toutes sortes de marques qui trahissent nos agissements ; en cela, ils nous tracent. Les opérateurs téléphoniques savent où nous sommes dès que nous allumons nos téléphones portables ; les services de l'assurance maladie disposent d'informations sur notre santé, en particulier de nos visites chez les médecins et des remèdes que nous nous sommes procurés en pharmacie ; les banques accèdent à nos achats et, surtout, aux endroits où nous nous trouvions lorsque nous avons payé avec nos cartes de crédit etc. On engrange ces « miettes » de nos vies dans des dispositifs de stockage

d'information, que l'on appelle communément des mémoires informatiques, pour les exploiter ensuite. L'économie du web repose en grande partie là-dessus. Le profilage nécessaire tant à la publicité ciblée qu'à la recommandation commerciale ou à la propagande politique, y fait appel. Des policiers y recourent aussi ; et il en va de même de nombreux cybercriminels ou maîtres chanteurs, voire de services de renseignements. Les fabricants de systèmes d'exploitation d'ordinateurs, par exemple la société Google qui développe le système d'exploitation Android ou la société Apple avec l'iOS, traquent les activités des utilisateurs et conservent leurs données personnelles. Une option par défaut du système d'exploitation Android vantée comme assurant la sécurité des utilisateurs en cas de vol, enregistre et conserve sans limitation de durée l'ensemble des déplacements individuels de chacun, à la minute près !

Il existe aussi d'autres utilisations des traces moins sujettes à controverse, pour l'écologie ou la santé. Ainsi, les utilisera-t-on bientôt pour établir le bilan carbone de nombreuses activités, en particulier de l'agriculture, ou par souci prophylactique, pour prévenir des crises graves à partir de capteurs physiologiques chez des patients souffrant d'affections chroniques, par exemple de diabète, voire même pour anticiper des risques de maladies.

Aujourd'hui, avec la crise sanitaire due à la pandémie de CoViD-19, on cherche à tracer les contacts des personnes malades pour deux raisons au moins : les avertir d'une possible contagion, afin de les soigner et de les isoler, et procéder à des études épidémiologiques, pour mieux connaître les mécanismes de transmission de la maladie. Doit-on s'en inquiéter et condamner ce traçage, ou au contraire l'encourager, et sous quelles conditions ? Telles sont les questions que nous allons aborder ici.

Dangers, utilité et nécessité

Que ses finalités soient bienveillantes, comme pour la protection de la santé des individus, de l'état sanitaire ou de l'environnement, qu'elles soient mercantiles, policières ou politiques, voire vraiment malveillantes, telles l'espionnage et la cybercriminalité, le traçage fait irruption dans la vie privée. Certains craignent qu'il enfreigne les droits fondamentaux, en particulier le droit d'aller et venir, puisque nos déplacements sont pistés, le droit à la liberté de pensée, de conscience et de religion, car on connaît nos lectures et nos comportements, ou le droit à la liberté de réunion, du fait que l'on recense également nos fréquentations.

Pour autant, il n'y a là aucune fatalité : la recension et le stockage d'informations sur nos mouvements, nos goûts, nos prises de position ou nos contacts ne nous ôtent pas nécessairement notre liberté de mouvement, de pensée ou de réunion. La contrainte ne s'exerce que lorsque les acteurs qui récupèrent et exploitent les informations le font à l'insu des personnes, sans recueillir leur consentement, en vue d'un usage malveillant.

Or, il existe des situations où beaucoup s'accordent sur l'utilité du traçage, voire même sur sa nécessité. Ainsi en va-t-il pour assurer la sécurité des personnes, qu'il s'agisse de la protection policière contre les actes terroristes ou simplement délictueux, ou encore de la prévention sanitaire pour anticiper les risques, qu'ils soient individuels ou collectifs, et lutter contre les crises sanitaires. À cela s'ajoutent les questions écologiques et alimentaires : le traçage de l'activité des agriculteurs et des éleveurs nous renseigne sur le coût des produits pour l'environnement, en particulier sur leur bilan carbone, et sur leur origine. Cela aidera aussi les citoyens responsables à mieux maîtriser leur alimentation. Plus généralement, l'État de droit doit recourir à toutes sortes de traçages pour assumer ses attributions régaliennes tant en matière de sécurité intérieure, que de santé publique, d'éducation, de finances, etc. Enfin, soulignons que le traçage assure la transparence, vertu considérée comme éminente dans le monde contemporain où l'opinion publique condamne tant l'opacité que le secret et devrait donc recommander le traçage.

Pour tirer parti des bénéfices du traçage, sans souffrir de ses inconvénients, il faut s'assurer que les informations personnelles recueillies ne se retourneront pas contre les personnes, autrement dit que leurs possesseurs n'en abuseront pas. À cette fin, un certain nombre de conditions doivent être respectées ; elles portent sur :

a. l'identification claire des différents acteurs qui recueillent les traces, les conservent et les exploitent
b. l'accord des intéressés sur la captation et les différentes utilisations prévues de leurs données personnelles
c. la transparence dans les différentes utilisations, qui doivent être explicitées de façon compréhensible
d. la possibilité pour les personnes de donner leur accord individuel à certaines utilisations seulement, sans être obligées d'accepter toutes les utilisations

e. le respect de la vie privée, en particulier l'absence de divulgation à des tiers sans une autorisation explicite qui, là encore, doit faire l'objet d'une demande claire et dissociée des autres demandes

Ceci signifie que les opérateurs chargés de recueillir, d'agréger et de traiter les traces doivent être des acteurs de confiance soumis à un certain nombre de contrôles de la part des citoyens et justiciables des infractions aux lois devant des cours reconnues.

Application de traçage pour contenir la pandémie de CoViD-19

Mis en place le 10 mars 2020 pour éclairer le gouvernement tant sur la pandémie que sur les actions requises pour en limiter les effets, le conseil scientifique Covid-19[1] s'est très tôt interrogé sur la stratégie à adopter à la fin du confinement pour éviter un rebond de l'épidémie. S'inspirant des expériences conduites avec succès dans les pays d'Asie du Sud-Est, tout particulièrement en Chine, en Corée du Sud et à Singapour, il a travaillé sur les stratégies à adopter. Outre le maintien des mesures de distanciation sociale bien connues de tous aujourd'hui, il préconisait des tests massifs, une mise en quarantaine des porteurs du virus et, surtout, un repérage des personnes avec qui ces derniers auraient pu entrer en contact prolongé avant d'être identifiés comme contagieux. Ce dernier volet de la stratégie tient à ce que, particularité de cette maladie, des patients restent peu symptomatiques (ce que l'on appelle « paucisymptomatique ») voire asymptomatiques plusieurs jours avant que la maladie ne se déclare, au cas où elle se déclare, tout en étant déjà susceptibles de contaminer les autres. Il convient donc de mener l'enquête auprès des patients avérés afin de retrouver les personnes avec qui ils ont été en contact, pour les tester au plus vite et les isoler si nécessaire, afin d'éviter, autant que faire se peut, la propagation du virus. De plus, il est bon, pour assurer la protection des populations, de procéder à des études statistiques afin de connaître les conditions de contamination : écoles, universités, lieux de convivialité, etc.

Il a été décidé de recourir aux médecins généralistes pour recenser les contacts auprès des patients et à des auxiliaires médicaux regroupés en corps appelés brigades, pour interroger les contacts, les inciter à se tester et, au cas où ils présenteraient des symptômes manifestes, les

[1] L'ensemble des rapports transmis par le conseil scientifique présidé par Jean-François Delfraissy est accessible publiquement sur le site du ministère de la Santé, https://solidarites-sante.gouv.fr/actualites/presse/dossiers-de-presse/article/covid-19-conseil-scientifique-covid-19

enjoindre à aller se faire soigner et mener des enquêtes auprès d'eux afin de connaître les conditions de la contamination. Enfin, prenant modèle sur ce qui a été fait en Asie, le comité scientifique a suggéré au gouvernement d'utiliser les téléphones portables pour tracer automatiquement, avec les ressources du numérique, les contacts de chaque personne.

Caractéristiques des applications de traçage

Dès que l'idée de tels dispositifs numériques a été émise, beaucoup s'en sont émus, craignant leur caractère potentiellement intrusif et les conséquences pour la vie privée, en particulier pour la liberté de réunion, puisque ces dispositifs enregistrent continûment nos fréquentations. En accord avec le ministère de la Santé, les scientifiques français chargés de réfléchir à leur conception, en particulier ceux d'Inria, se sont demandé comment cela pourrait rester compatible avec nos valeurs et nos lois. Un certain nombre de choix ont donc été faits :

- absence de localisation, en particulier pas d'utilisation du GPS, ni même des cellules du réseau téléphonique ;
- repérage automatique des contacts entre les téléphones mobiles avec les ondes dites Bluetooth conçues pour des communications à très courte distance (moins de cinq mètres) entre des appareils connectés, montres, écouteurs, etc.
- stockage des contacts de façon totalement anonyme, en utilisant des techniques de cryptographie ;
- lorsqu'une personne se révèle porteuse du virus, à l'issue d'un test, envoi anonyme, à tous ceux qui ont été en contact avec cette personne, et qui sont donc susceptibles d'avoir été infectés par elle, d'un message les enjoignant à subir un test et, si ils éprouvent des symptômes, à prendre contact avec un médecin.

On notera qu'à condition de ne pas être piratés, des dispositifs qui satisfont ces critères protègent bien plus la vie privée que les brigades mentionnées plus haut, car, dans le cas de telles applications numériques, l'identité des personnes malades n'est jamais transmise de façon explicite, alors que le dispositif humain demande de connaître les personnes contagieuses susceptibles d'être à la source des probables contaminations, d'enregistrer leur identité sur une base de données nominatives et de solliciter un membre des brigades, qui n'est pas médecin, et donc pas tenu par le serment d'Hippocrate afin qu'il les interroge.

Réflexions sur les différentes architectures des applications de traçage

Des réflexions analogues se sont poursuivies dans différents pays européens, tous sensibles aux mêmes impératifs de protection de la vie privée. Deux architectures informatiques sont alors apparues comme envisageables : une architecture dite, un peu sommairement, « centralisée »[23] en ce sens que les identifiants cryptés des personnes ayant été en contact avec un individu contagieux sont transmis par intervalles réguliers, de l'ordre de la journée, à un ordinateur central qui se charge ensuite, en cas de test positif d'un individu, d'envoyer des notifications aux personnes susceptibles d'avoir été en contact avec lui ; une architecture qualifiée de « décentralisée »[5], comme le protocole DP-3T :*Decentralized Privacy-Preserving Proximity Tracing* déployé par un consortium piloté par les sociétés Apple et Google, parce que les téléphones portables stockent, toujours sous forme cryptée, l'ensemble des identifiants des contacts, et les envoient automatiquement lorsque le détenteur du téléphone se déclare porteur du virus. Bénéfice supplémentaire de l'architecture centralisée, celle-ci procure à un État une vision d'ensemble de l'évolution de la pandémie, sans qu'il ait besoin d'accéder à l'identité des personnes, puisque les identifiants restent cryptés. L'architecture décentralisée laisse l'opérateur téléphonique maître des données, car celles-ci restant disséminées sur les téléphones individuels, il en conserve l'accès potentiel. En cas de déclaration de maladie, le téléphone envoie de lui-même les messages aux personnes ayant été en contact avec l'individu contagieux. Bien que cette solution évite de les stocker sur un ordinateur central, elle n'apparaît pas plus sûre, car n'importe quel pirate judicieux serait en mesure de les repérer. Vu ce qui vient d'être dit, on conçoit que la France, pays de tradition jacobine, ait choisi une architecture centralisée pour la mise en place de l'application StopCovid. Les pays du nord de l'Europe, pour des raisons pragmatiques venant de la décision d'Apple de ne pas ouvrir son système d'exploitation à un autre protocole que le sien, optèrent pour le protocole DP-3T.

---

[2] Par exemple le protocole protocole Robert : *ROBust and privacy- presERvingproximityTracing* mis au point conjointement par Inria en France et le Fraunhofer en Allemagne. Cf. https://www.inria.fr/fr/publication-du-protocole-robert

[3] On peut aussi lire avec profit une description des choix de conceptions du protocole ROBERT par le président d'Inria, Bruno Sportisse : https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux

[5] Pour une description du protocole DP-3T, lire https://medium.com/@OpenTrace/review-of-new-apple-and-google-contact-tracing-protocol-7696c9203967

Reprenons maintenant les critères requis pour s'assurer que le système de traçage satisfasse les critères a, b, c, d, e mentionnés précédemment :

a. Dans le cas d'une architecture centralisée mise en œuvre par un État, il n'existe qu'un seul acteur, bien identifié ; dans le cas d'architectures décentralisées, les opérateurs téléphoniques et les fabricants de systèmes d'exploitation interviendront de façon concurrente ; ils seront connus, mais du fait de leur multiplicité et, surtout, de l'extraterritorialité de certains d'entre eux, il sera difficile de s'assurer qu'ils offrent les garanties requises.
b. L'accord des intéressés peut être acquis dans les deux architectures, puisque dans l'une comme dans l'autre, tant l'installation que l'activation ou la désactivation de l'application sont volontaires.
c. La transparence des différentes utilisations faites des données personnelles dépend de l'opérateur
d. La possibilité de donner son accord à certaines utilisations et pas à toutes, dépend du contrat qui lie opérateurs et utilisateurs
e. Enfin, l'absence de divulgation de l'information sans autorisation explicite dépend aussi de l'opérateur

Pour s'assurer que les conditions b, c, d et e soient vérifiées, il faut que les opérateurs impliqués soient justiciables devant des cours nationales ou supranationales. Si notre État reste un État de droit, s'il se soumet aux lois que le parlement a votées, s'il protège la base centrale de données, tout en conservant l'anonymat des données, et s'il demeure loyal, la solution qualifiée de centralisée paraît préférable, car plus fiable, puisqu'elle limite les possibilités de fuite. Si l'État en profite pour renforcer l'appareil policier et la surveillance de la population, alors la solution décentralisée est préférable, à condition toutefois que l'on puisse faire confiance aux opérateurs téléphoniques et, surtout, aux maîtres des systèmes d'exploitation de nos téléphones, comme Apple ou Google. Or, ces derniers échappant en grande partie aux législations nationales des États européens, on peut craindre qu'ils sauront se jouer des lois à leur avantage, voire qu'ils passeront outre sans vergogne.

Qui plus est, le récent CLOUD-Act entré en vigueur en 2018 aux États-Unis autorise les instances de l'État fédéral américain à contraindre les fournisseurs d'accès internet établis sur le territoire américain à leur livrer, sur requête d'un juge, les données stockées sur leurs serveurs

qu'ils soient situés aux États-Unis ou ailleurs. En clair, cela signifie que des juges américains peuvent exiger d'avoir accès aux données de communication des téléphones Apple ou Google, même si celles-ci viennent de l'étranger. Autrement dit, même si, avec le protocole « décentralisé » proposé par Apple et Google, les États européens n'auront pas accès aux données des européens, les institutions américaines auront toujours la possibilité d'y accéder.

Traçage de la peur

Au printemps 2020, les applications de traçage suscitèrent l'effroi dans l'opinion publique, avant même qu'elles existent en Europe. On s'inquiétait alors de la probable main mise d'un État policier sur les données personnelles les plus sensibles que sont les données de déplacements et les données de santé. Un nombre considérable d'alertes furent lancées. Beaucoup tentèrent d'avertir, pour reprendre les mots de Christiane Taubira dans une tribune courageuse[6], du « grignotage » de nos libertés. De nombreux intellectuels et de non moins nombreux hommes politiques de tous bords, hérauts des libertés publiques, se mobilisèrent pour la défense de ces mêmes libertés. Selon eux, plus que la CoViD-19, nous devions craindre l'asservissement par un pouvoir résolument autoritaire. Mieux valait mourir debout que de vivre en esclavage !

Ces données de traçage ne révélaient-elles pas notre état de santé, en particulier une probable contagiosité ? Dans ce cas, ne devions-nous pas craindre que l'État en profite pour exercer des discriminations ? D'autres évoquaient le suivi continu des déplacements des personnes et surtout de leurs fréquentations, voire la transmission des coordonnées des personnes présentes sur nos carnets d'adresse. Enfin, tous s'épouvantaient de ce que la licence donnée à l'État durant la pandémie ne servît de prétexte à une banalisation du traçage. On conçoit qu'échaudés par la prolongation indéfinie de l'état d'urgence contre le terrorisme dans notre pays, avec des contrôles incessants et humiliants à l'entrée de toutes les institutions, beaucoup s'alarment de ces mesures et de leur possible prorogation. On sait aussi la vulnérabilité de tout système informatique, fût-il protégé par des techniques de cryptographie. En cas d'attaques et de piratage, nos données personnelles auraient été divulguées à tous les vents.

---

[6] France-Info, 13 avril 2020, https://www.francetvinfo.fr/sante/maladie/coronavirus/tracking-contre-le-coronavirus-non-au-moindre-grignotage-de-liberte-alerte-christiane-taubira_3913177.html

Ceci étant, les craintes d'exploitation massive des données de traçage par l'État paraissent, à la réflexion, assez incongrues dans un pays où la Sécurité sociale trace déjà, avec les cartes vitales et les bases de données de l'assurance maladie, l'état de santé des patients, en particulier leurs visites chez les médecins, les médicaments achetés, leurs hospitalisations et, dans le cas de la CoViD-19, ce qui n'est pas négligeable, leurs vaccinations. Pourquoi imaginer qu'avec des applications de traçage aussi protégées que nous l'avons expliqué, l'État chercherait à utiliser ces données-ci, pour accroître son emprise sur la population, alors qu'il dispose déjà de données plus complètes, et ce en quantité beaucoup plus considérable ?

Quant au risque de piratage des données de traçage, il n'est pas pire que le risque de piratage des cartes vitales ou des transactions bancaires. Enfin, les opérateurs téléphoniques et les systèmes d'exploitation des téléphones portables disposent d'informations de localisation qui nous pistent déjà.

Ajoutons à cela qu'en vertu du même CLOUD-Act mentionné plus haut, le choix de Microsoft comme opérateur du Health Data Hub permet à l'État américain de préempter l'intégralité des données de santé des français, sans que cela ne mobilise grand monde en France. Pourtant, à l'époque où cette loi a été votée, le président des États-Unis n'apparaissait pas être un parangon des vertus démocratiques. De plus, il paraît étrange de craindre plus les dérives du pouvoir démocratique de son propre pays que celle d'un État étranger.

Les inquiétudes suscitées par les applications de traçage demandent donc à être relativisées. C'est d'ailleurs ce que les français comprirent spontanément à l'automne 2020. Rappelons que l'application StopCovid, sur laquelle s'étaient cristallisées toutes les peurs au printemps 2020, n'a été téléchargée qu'à moins de deux millions d'exemplaires dans le courant de l'été. Or, après les grandes vacances, une application très semblable, baptisée TousAntiCovid, se substitua à StopCovid, sans provoquer les mêmes craintes. Seuls changements notables, le nom et l'adjonction d'un certain nombre de fonctionnalités, dont, par exemple, les facilités d'accès aux attestations de sortie. Pourtant, plus personne ne s'opposa vraiment à ce nouveau logiciel de traçage. Plus aucun article ne le mentionna à la rentrée. Les hérauts médiatiques de nos libertés n'en parlèrent plus. Et, peut-être est-ce pour cela que, selon un article de presse du 10 mars

2021[7], l'application téléchargée à plus de 13 millions d'exemplaires, a alerté plus de 100.000 cas contacts. Bref, de même que la nuit porte conseil, l'été aussi…

[7] Raphaël Grably, *Depuis son lancement, l'application TousAntiCovid a alerté 100.000 cas contacts*, 10 mars 2021, BFM Business, tech, https://www.bfmtv.com/amp/tech/depuis-son-lancement-l-application-tous-anti-covid-a-alerte-100-000-cas-contacts_AN-202103100026.html