Note de réflexion applications Covid-19

- 29 mai 2020 -

Jade Vergnes, étudiante en M1 à Sciences Po (EMI)
Charles-Eric de Benoît d'Entrevaux, étudiant en M1 à Sciences Po (EMI)
Christine Balagué, Professeur, Institut Mines-Télécom Business School, Titulaire de la chaire Good in Tech (www.goodintech.org)

Synthèse

La présente note a pour objectif de dresser un état des lieux des controverses concernant les applications de traçage mises en place dans un contexte pandémique. **L'objectif est triple** : **synthétique** - en rassemblant les diverses informations, arguments et acteurs -, **analytique** - en mettant ces informations factuelles à l'épreuve d'un questionnement conceptuel sur les notions fondatrices de nos sociétés démocratiques : la tension entre liberté et sécurité, le contrat social, le droit fondamental au respect de la vie privée, etc -, et enfin, **prospectif** - en établissant quatre scénarios concernant l'application StopCovid, mise en place par le gouvernement français -.

L'étude rassemble un **tableau comparatif des différentes formes d'applications** développées et utilisées dans le monde. Au travers d'une étude approfondie de la stratégie française, **une carte heuristique** détaille **les arguments favorables et défavorables au lancement de l'application StopCovid**, ainsi que les acteurs qui soutiennent ces positions.

Enfin, **quatre scénarios possibles sont développés sous le prisme du cas français** : le scénario du lancement de l'application StopCovid, le scénario du retrait de l'application StopCovid, la voie libre à une application contrôlée par Google et Apple et des scénarios alternatifs. Chacune de ces pistes rassemble les bénéfices et les dangers pour les individus et prend en compte les enjeux politiques, technologiques, sanitaires et éthiques.

Le quatrième et dernier scénario a pour vocation d'illustrer **des recommandations stratégiques** afin de lutter au mieux contre la propagation de la pandémie tout en étant intransigeants sur le respect des libertés et droits fondamentaux. Il propose la mise en avant d'**une stratégie *stuff and staff*** plus efficace, de **renforcer la transparence**, les processus démocratiques et l'éducation civique sur les risques technologiques, et enfin, prône une **coordination européenne** afin de porter la vision d'une société éminemment numérique au coeur de laquelle les droits individuels sont préservés.

Sommaire

I. Le contexte

De quoi parle-t-on ?

Le contexte sanitaire

Fin 2019, le virus Covid-19 apparaît dans la ville chinoise de Wuhan et se propage en quelques mois dans la majorité des pays du monde. Le 30 janvier 2020, l'état d'urgence de santé publique à portée internationale est déclaré par l'*Organisation mondiale de la santé* (*OMS*). Au total, il est estimé que le virus fait environ 302 000 morts[1] dans le monde à la date du 15 mai 2020. Une grande partie des pays suivent une stratégie de confinement des populations afin de limiter les interactions sociales et, ainsi, endiguer la propagation du virus. Cependant, au terme de cette période d'arrêt partiel ou total des activités, ayant d'ors et déjà de fortes conséquences économiques, sociales et psychologiques, l'étape du déconfinement s'avère cruciale afin d'éviter ce que tous les gouvernements craignent : une seconde vague épidémique et un nouveau confinement.

Les États mettent donc en place une série de mesures, comme la production massive de masques et de tests, afin de protéger les transmissions et de détecter au plus vite les personnes contaminées. Parmi cette palette d'outils apparaît le développement d'applications de traçage des contacts humains qui poursuivent deux objectifs : le premier, celui de mesurer la propagation du virus et le taux de circulation, le second, d'alerter les personnes au plus tôt qu'elles sont potentiellement porteuses du virus car elles ont été exposées à quelqu'un de malade. En effet, le virus prend souvent des formes asymptomatiques et se déclare en moyenne cinq jours après la contamination, ce qui augmente la contagiosité du virus.

Le contexte politique

Cette crise sanitaire plonge également les États dans un contexte politique tendu. La situation met en lumière des institutions mal préparées à une pandémie et trop peu réactives aux signes avant coureurs. La courbe exponentielle du nombre de cas de Covid-19 fait craindre une explosion du système hospitalier face à l'afflux massif de malades. C'est pourquoi, dans certains États, la stratégie de confinement est choisie, instaurant ainsi un système de restrictions des libertés inédit. Les citoyens sont enfermés chez eux pendant plusieurs mois, tous les regroupements sont interdits et les sorties ne sont permises qu'avec une attestation dérogatoire. Toute infraction à ces règles est punie d'une amende. Cette réponse à la pandémie peut être perçue comme une priorisation de la sécurité des individus sur leur liberté : c'est pour votre bien et celui de vos proches que vous renoncez à vos libertés.

Le contexte technologique

Parallèlement, cette crise mondiale accélère drastiquement le processus de numérisation des activités humaines : télétravail, cours en ligne, activités culturelles virtuelles - comme des musées -, appels de groupes personnels, etc. A la question « comment continuer d'entretenir une vie normale tout en étant privés du monde extérieur ? », le numérique semble être la solution alternative au monde réel devenu invivable. En effet, la pandémie Covid-19 surgit dans un contexte d'explosion de la production de données dans le monde : quand, en 2010, était produit 1 zettabyte par an - 10^{21}, soit cinq fois ce qui n'a jamais été écrit sur terre -, on estime qu'en 2025, on atteindra 140 zettabytes. Ainsi, le confinement représente une aubaine pour le développement de nouvelles technologies : il permet une expérimentation accélérée et à grande échelle de certains outils numériques. Dans un contexte favorable au solutionnisme technologique, les responsables politiques et chercheurs décident d'aller plus loin et de mettre en place des applications de traçage des contacts humains.

[1] MOYOU, E. « Nombre de décès dus au coronavirus par pays du monde 15 mai 2020 », *Statista*, 15/05/2020. Disponible sur <https://fr.statista.com/statistiques/1101324/morts-coronavirus-monde/>

Le dilemme de la sécurité contre la liberté au coeur du débat

La teneur du débat : le crainte d'une atteinte aux libertés fondamentales et à la vie privée

Alors que les premières mesures de restriction des libertés dans le cadre du confinement sont acceptées sans trop de protestations, à l'exception des États-Unis, le débat émerge et se cristallise autour de la question des applications de traçage. Perçues comme un progrès technique et outil indispensable pour lutter contre la propagation du virus par certains, d'autres s'alarment quant aux risques majeurs pour le respect de la vie privée des individus. En filigrane du débat, c'est la peur d'une surveillance de masse instaurée sous couvert de crise, en conduisant peu à peu à la banalisation de certaines technologies. Les mots de Simone de Beauvoir résonnent avec force : « *n'oubliez jamais qu'il suffira d'une crise politique, économique ou religieuse pour que les droits des femmes soient remis en question* ». Une injonction qui s'applique tout autant aux libertés et droits fondamentaux durement acquis au cours des siècles. Le confinement, la généralisation de l'usage du masque et la mise en place d'une application de traçage convoquent un imaginaire qui fait écho aux scénarios dystopiques de notre siècle : du « *Big Brother is watching you* »[2], expression utilisée pour qualifier la surveillance de masse portant atteinte aux libertés fondamentales et à la vie privée des individus depuis la publication de *1984* de George Orwell, jusqu'aux dystopies technologiques, notamment incarnées par la série populaire *Black Mirror*[3], certaines similitudes effraient[4].

Nous sommes face à un dilemme : préférons-nous la sécurité à la liberté ?

S'il est encore trop tôt pour considérer les applications de traçage tout droit sorties d'un scénario de science-fiction, la singularité et le caractère exceptionnel de cette crise nous obligent à tenir des débats sur les valeurs fondamentales qui régissent nos sociétés. En effet, les innovations technologiques mettent au défi nos priorités et nous remettent face à l'éternelle question : préférons-nous la sécurité à la liberté ? Un débat qui opposait déjà Rousseau et Tocqueville, a traversé le XXème siècle et, plus récemment, à fait couler beaucoup d'encre suite à la multiplication d'attentats à partir de 2015.

La pandémie du Covid-19 et la mise en place d'applications de traçage poussent à se poser cette même question : jusqu'où sommes-nous prêts à aller pour assurer notre sécurité ? « *M'enfermer pour mon bien ? Non merci !* » scande André-Comte Sponville, quand Francis Wolff analyse plutôt la situation comme « *le signe d'un progrès moral de l'humanité* »[5]. Il semble difficile de choisir entre ces deux valeurs tout aussi précieuses au respect de la dignité humaine. Si elles ne s'opposent pas frontalement, leur articulation provoque parfois des tensions, créant des situations de dilemme décisionnel. Sans proposer une vision manichéenne de la situation, opposant une vision pro-libérale contre pro-sécuritaire, une autre technophile contre technophobe, il est nécessaire de se pencher sur les points techniques des applications de traçage et les controverses rencontrées afin de considérer la solution pour trouver le juste équilibre entre sécurité et liberté dans le cadre de la lutte contre la propagation du virus.

A ces questions, les pays du monde entier apportent une réponse distincte, en développant des applications utilisant des technologies et protocoles divers.

---

[2] ORWELL, Georges. *1984*. 1949.

[3] Black Mirror est une série télévisée britannique, créée par Charlie Brooker, dont chaque épisode est une dystopie technologique.

[4] UNTERSINGER Martin. « StopCovid, une application de traçage passée en deux mois de l'idée dystopique à l'assemblée », *Le Monde*, 27/04/2020. Disponible sur <https://www.lemonde.fr/pixels/article/2020/04/27/stopcovid-une-application-de-tracage-passee-en-deux-mois-de-l-idee-dystopique-a-l-assemblee_6037924_4408996.html>

[5] SPONVILLE, André-Comte ; WOLFF, Francis. « Préférons-nous la santé à la liberté ? », *Philomag*, 09/05/2020. Disponible sur <https://www.philomag.com/lactu/dialogues/andre-comte-sponvillefrancis-wolff-preferons-nous-la-sante-a-la-liberte-43148>

Etude comparative : quelles applications dans quels pays ?

En effet, les applications de traçage sont aussi diverses que les objectifs poursuivis. Afin de dresser un état des lieux des différentes technologies mises en place par chaque pays, nous avons constitué un tableau comparatif au niveau international.

Ce tableau n'est pas exhaustif et ne prend pas en compte les initiatives à l'échelle régionale. Nous nous sommes concentrés sur les applications de traçage, mais d'autres technologies, à l'instar des drones[6] ou de suivi bancaire, ont pu voir le jour dans différents pays du monde afin de faire respecter le confinement et de contrôler le déconfinement. Une grande partie des initiatives technologiques mondiales ont été collectées de manière collaborative dans ce tableau : https://ethercalc.org/gq47xdrzw99y.

[6] La Quadrature du Net. « L'attaque des drones », *La Quadrature*, 01/04/2020. Disponible sur <https://www.laquadrature.net/2020/04/01/covid-19-lattaque-des-drones/>

Pays	Nom de l'application	Modalités de la technologie de traçage	Finalité recherchée	Technologie utilisée	Dirigeant	Détails	Stade de développement	Sources
Chine	Close Contact Detector App	Application, objets connectés, vidéo surveillance	Traçage des contacts humains	Reconnaissance faciale, géolocalisation	L'État et la *China Electronics Technology Group Corporation* (*CETC*)	Une application génère des QR codes dont la couleur varie en fonction de l'état de santé de la personne : vert, jaune, rouge. S'il est jaune/rouge, la personne doit être mise en quarantaine. Cette application récupère : la géolocalisation, l'adresse postale, les numéros de téléphone et de pièce d'identité de l'utilisateur. Il conditionne l'accès aux services.	Obligatoire pour accéder aux services. Mis en place dès le début du déconfinement.	• https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
Singapour	TraceTogether	Application	Traçage des contacts humains	*Bluethooth*	État (ministères santé et technologies)	Application qui identifie les personnes ayant été en contact *Bluetooth* plus de 30 minutes avec un malade. Sur base du volontariat et pseudonymisation.	Utilisée : 620 000 personnes ont installé l'application en 3 jours.	• https://www.computerweekly.com/news/252480501/Singapore-government-to-open-source-contact-tracing-protocol • https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf
Hong Kong	StayHomeSafe	Bracelets électroniques, applications	Respect du confinement	*Bluethooh*, reconnaissance faciale, géolocalisation	État (ministères santé et technologies)	À Hong Kong, les autorités ont doté toutes les personnes revenant de l'étranger d'un bracelet électronique, similaire à ceux utilisés en cas de peines judiciaires. Celui-ci était ensuite relié à une application devant être téléchargée sur un smartphone. Cette application peut envoyer un message d'alerte en cas de sortie du périmètre programmé.	Obligatoire (6 mois de prison encourrus si la quarantaine est rompue). Néanmoins, sur les 6000 bracelets, seulement 1/3 ont été activés.	• https://www.businessinsider.fr/us/hong-kong-wristbands-tracking-people-in-coronavirus-quarantine-2020-2 • https://www.theguardian.com/commentisfree/2020/mar/21/smartphones-could-help-track-coronavirus-but-at-what-cost
Corrée du Sud	Confirmed Patients Movement Path	Application et vidéo surveillance	Traçage des contacts humains, respect du confinement	Reconnaissance faciale, géolocalisation	État	Données récoltées sur les téléphones et cartes bancaires. Les amendes pour rupture de quarantaine sont lourdes et s'accompagneront bientôt de la menace d'une peine de prison. Un site du gouvernement publie la localisation des malades.	Utilisée	• https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives
Israël	HaMagen (retrait de l'application fin avril)	Application	Traçage des contacts humains, respect du confinement (puis retrait)	Géolocalisation	Etat - données traitées par le *Shin Bet*, service de sécurité intérieure, utilisent les moyens anti-terroristes pour suivre les déplacements des porteurs du virus grâce à plus de 70 mesures d'exception (un record).	Carte d'identité nationale, numéro de téléphone, historique des crédits, des voyages et des contacts. Les données de circulation des malades sont publiques.	Utilisée puis retrait le 27 avril 2020, car jugée trop dangereuse pour le respect de la vie privée par la Cour Suprême israélienne.	• https://www.marianne.net/monde/une-severe-violation-du-droit-constitutionnel-la-vie-privee-en-israel-la-cour-supreme-dit-non • https://medium.com/proferosec-osm/hamagen-application-fighiting-the-corona-virus-4ecf55eb4f7c
Russie		Application, caméras de reconnaissance faciale (plus de 170 000), puces cartes bancaires	Traçage de la diffusion du virus, respect du confinement	Géolocalisation, reconnaissance faciale, QR code, localisation carte bancaire	État (à Moscou notamment)	La géolocalisation permet de signaler à des personnes ayant été en contact avec des malades. Pas d'anonymisation des données. Le système de reconnaissance faciale est développé massivement. À partir de la géolocalisation du téléphone et de la carte bancaire, les autorités imposent aux personnes ayant été à moins de 2 mètres pendant plus de 10 minutes d'un malade de se mettre en quarantaine.	Utilisée et obligatoire pour les personnes infectées.	• https://www.reuters.com/article/us-china-health-moscow-technology/moscow-deploys-facial-recognition-technology-for-coronavirus-quarantine-idUSKBN20F1RZ?feedType=RSS&feedName=technologyNews • https://edition.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html

Pologne	Home Quarantine	Application	Respect du confinement	Reconnaissance faciale, géolocalisation	État	Obligation pour les personnes revenant de l'étranger d'installer l'application de traçage : doivent envoyer des selfies sous 20 minutes si on leur demande pour confirmer qu'ils respectent les consignes. Contrôle de police en cas de retard ou refus.	Utilisée et obligatoire pour les personnes infectées.	• https://www.privacyinternational.org/examples/3473/poland-app-helps-police-monitor-home-quarantine
Suisse	Data Analytics	Application	Suivi de la distance sociale, pas de traçage des contats humains	Localisation des cartes SIM par triangulation des antennes	*Swisscom* (opérateur téléphonique) communique des données à l'*Office fédéral de la santé publique* (État).	Une application pour respecter la distance sociale dans les places publiques. L'objectif est de limiter les attroupements. L'opérateur communique aux autorités fédérales lorsque plus de 20 téléphones se trouvent dans un espace de 100m2. Informations transmises 24 heures après. Les données ne peuvent pas être utilisées pour d'autres objectifs, les investigations criminelles incluses. Données pseudomysées. Les utilisateurs peuvent refuser que leurs données soient analysées.	Utilisée : 6 300 000 utilisateurs de Swisscom.	• https://www.letemps.ch/economie/swisscom-aidera-confederation-detecter-attroupements-via-telephones
Espagne	Pas d'application nationale pour le moment							
Allemagne		Application	Traçage des contacts humains	*Bluetooth* (protocole décentralisé)	*Google*/*Apple* avec l'État	Application qui renseigne les contacts humains grâce à la technologie *Bluetooth*. Elle respecte la pseudonymisation des données et les règles européennes régies par le *RGPD*.	Pas encore lancée.	• https://www.lepoint.fr/sciences-nature/application-de-tracage-l-allemagne-mise-finalement-sur-apple-et-google-26-04-2020-2372940_1924.php
Allemagne	Corona-Datenspende	Montres et bracelets connectés	Détection des symptômes	Technologies fitness : pulsation cardiaque, température, agitation du sommeil	État en partenariat avec la start-up de santé tech *Thryve*	Détecte la température et l'agitation du sommeil à partir d'informations médicales (taille, poids, sexe, pulsation, habitudes) et l'adresse de la personne, afin d'alerter d'une contamination possible au Covid-19. Création d'une carte interactive en ligne qui permet, en la croisant avec d'autres données, d'évaluer la prévalence des infections au niveau du code postal.	Lancée le mardi 7 avril 2020. Utilisée sur base du volontariat. Objectif : 100 000 utilisateurs.	• https://www.reuters.com/article/us-health-coronavirus-germany-tech/germany-launches-smartwatch-app-to-monitor-coronavirus-spread-idUSKBN21P1SS Lien pour l'application : https://corona-datenspende.de/
Italie	Immuni	Application	Traçage des contacts humains et cartographie de l'épidémie	*Bluetooth* (protocole décentralisé)	État	L'application comprend deux volants : le premier consiste au traçage des contacts humain par Bluetooth, le second à récolter les informations médicales des utilisateurs, mise à jour quotidiennement, afin de tenir un journal clinique (sexe, âge, maladies passées, prise de médicaments). Sur base du volontariat et données pseudomysées.	Pas encore lancée. Pour être efficace, elle devra être utilisée par 60% des italiens.	• https://www.repubblica.it/politica/2020/04/16/news/coronavirus_scelta_l_app_per_il_tracciamento_dei_contagi_si_chiamera_immuni-254235342/ https://www.lesechos.fr/tech-medias/hightech/italie-polemique-autour-de-lapplication-de-tracabilite-du-covid-19-1196790
France	StopCovid	Application (application paneuropéenne PEPP-PT)	Traçage des contacts humains	*Bluethooh* (protocole centralisé)	Etat	L'application a pour objectif de tracer les contacts humains par la technologie *Bluetooth*. Sur base du volontariat et données pseudomysées.	Lancement le 2 juin 2020.	

II. Présentation de StopCovid et analyse des controverses sur les enjeux éthiques

De sa conception algorithmique à l'exploitation épidémiologique des résultats, en passant par l'utilisation de données d'utilisateurs, le projet d'application StopCovid suscite de nombreux débats. En retraçant le parcours de réflexion, production, utilisation et exploitation de l'application, il conviendra d'identifier les différentes controverses. Les positions des différents acteurs qui encadrent, conçoivent et/ou réfléchissent à cette application ne sont, en général, pas manichéennes. Elle revêtent bien souvent des formes multiples, aux conditions et garanties nombreuses.

Les différents acteurs et protocoles de l'application

Les différents acteurs qui travaillent à la conception technique de StopCovid

Le 8 avril 2020, les Ministres de la Santé et du Numérique, Messieurs Olivier Véran et Cédric O, ont annoncé le lancement d'une réflexion autour d'une application française dans le cadre d'une stratégie globale de déconfinement. Ce projet gouvernemental, qui associe acteurs publics et privés, est piloté par l'*Institut national de recherche en sciences et technologies du numérique* (*Inria*). Au sein de l'équipe-projet, on peut compter la présence des membres titulaires suivants :

- *ANNSI* : cybersécurité,
- *Capgemini* : architecture et codéveloppement *back-end*,
- *Dassault Systèmes* : infrastructure souveraine de données qualifiées SecNumCloud,
- *Inserm* : modèles de santé,
- *Lunabee Studio* : développement des applications mobiles,
- *Orange* : diffusion de l'application et interopérabilité,
- *Santé Publique France* : insertion et articulation de l'application dans la stratégie globale et suivi des contacts (« *contact tracing* »),
- *Withings* : objets connectés.

L'équipe-projet est chargée de concevoir techniquement l'application StopCovid en apportant leur expertise.

À ces membres titulaires du projet, s'ajoutent des contributeurs volontaires à titre individuel :

- Frédéric Arnoux : co-fondateur de *STIM*, *start-up* de stratégie et de management de l'innovation,
- Sylvain Chaillou : concepteur rédacteur *freelance*,
- Thomas Chappuis : consultant en innovation,
- Benjamin Duban : co-fondateur de *STIM*, *start-up* de stratégie et de management de l'innovation,
- Gabriel Hubert : développeur *full stack* chez *GAC Group*,
- Jules Leclerc : *CX* et *UX* designer *freelance,*
- Daniel Marhély : fondateur de *lovelee*, *Deezer*, *Blackpills*, et co-fondateur de *Shaki Shaki*.

et en tant qu'organisation :

- *AADIS* : entreprise spécialisée dans la pose d'alarme de sécurité et d'automatisme pour la maison ou les locaux professionnels.
- *Accenture / Octo* : conseil en transformation digitale des organisations,
- *Atos* : conseil en transformation digitale des organisations,
- *Bertin Technologies* : supervision dans l'innovation technologique et industrielle,
- *Bloom* : sensibilisation et médiation scientifique pour la conservation marine,
- *Coalition Network* : application de *contact tracing*,
- *C4Diagnostics* : nouvelle technologie pour le diagnostic de maladies infectieuses,
- *Enalees* : tests de diagnostic moléculaire pour les animaux de compagnie,
- Intersec : société de logiciels spécialisée dans les *Big Data* pour l'industrie des télécommunications, les entreprises, villes ou administrations,
- *Lifen* : solution de communication médicale,
- *NamR* : *start-up* en production de *data* originales et actionnables et en intelligence artificielle,
- *Sêmeia* : solution d'accompagnement de patients atteints de maladies graves ou chroniques,
- *Sia Partners* : conseil en management et en intelligence artificielle,
- *Sopra Steria* : services numériques et conseil en transformation digitale des organisations,
- *Thales* : groupe d'électronique spécialisé dans l'aérospatiale, la défense, la sécurité et le transport terrestre.

Ces personnes, physiques ou morales, ont manifesté leur volonté de participer au projet, dans la réflexion, création ou le test de l'application StopCovid.

Les débats protocolaires au sein de la communauté scientifique européenne

Aux côtés d'équipes allemandes, italiennes et suisses, les équipes de l'*Inria* ont publié conjointement, avec leur partenaire allemand du *Fraunhofer*, le protocole *ROBERT - ROBust and privacy-presERving proximity Tracing*[7]. Comme défini par les deux acteurs, il s'agit d' « *un protocole de suivi des contacts rapprochés, rigoureux et respectueux de la vie privée.* » Ce dernier évoque l'ensemble des réflexions sur l'architecture technique respectueuse des valeurs européennes. Toutefois, d'après les nombreuses critiques de la communauté scientifique, ces garanties ne semblent pas suffire.

En effet, le 19 avril 2020, 300 scientifiques experts du domaine, ont signé une alerte[8]. Ils s'interrogent sur la possibilité d'une surveillance généralisée de la société. Parmi ces signataires, Jacques Stern, médaille d'or du *CNRS* et inventeur de la cryptographie nationale.

D'autres chercheurs français, dont plusieurs travaillent à l'*Inria* ou au *CNRS*, poursuivent ces réflexions. Dans une analyse des risques à destination des non-spécialistes intitulée « Le traçage anonyme, dangereux oxymore »[9], ces spécialistes en cryptographie, présentent « *les détournements possibles d'une telle technologie, quels que soient les détails de sa mise en œuvre.* »

D'autres protocoles concurrencent le protocole *ROBERT*, comme le protocole *DP3T*. Ce dernier est décentralisé, tout comme l'est celui d'*Apple* et de *Google*. Dans un texte commun[10], les auteurs estiment qu'avec l'architecture centralisée du protocole des équipes de l'*Inria*, il y a un risque important d'être

[7] Inria ; Fraunhofer AIESEC. « ROBERT : un protocole de suivi des contacts respectueux de la vie privée », 18/04/2020. Disponible sur <https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-summary-FR.pdf>

[8] « Join Statement on Contact Tracing », 19/04/2020. Disponible sur <https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view>

[9] BONNETAIN, Xavier ; CANTEAU, Anne ; CORTIER, Véronique ; GAUDRY, Pierrick ; HIRSCHI, Lucca ; KREMER, Steve ; LACOUR, Stéphanie ; LEQUESNE, Matthieu ; LEURENT, Gaëtan ; PERRIN, Léo ; SCHROTTENLOHER, André ; THOMÉ, Emmanuel ; VAUDENAY, Serge ; VUILLOT, Christophe. « Le traçage anonyme, dangereux oxymore », *Risques-traçage*, 21/04/2020. Disponible sur <https://risques-tracage.fr/docs/risques-tracage.pdf>

[10] The DP-3T Project. « Security and privacy analysis of the document 'PEPP-PT: Data Protection and Information Security Architecture' ». 18/04/2020. Disponible sur <https://github.com/DP-3T/documents/blob/master/Security%20analysis/PEPP-PT_%20Data%20Protection%20Architechture%20-%20Security%20and%20privacy%20analysis.pdf>

désanonymisé ou de dévoiler son réseau de fréquentations. En réponse à cette critique, les auteurs de *ROBERT* ont ajouté un serveur intermédiaire qui mélange les codes reçus des personnes infectées par une technique appelée « *mix network* » avant de les transférer au serveur central. Cette démarche ne suffit pas : elle ne fait que déplacer le problème sur ce serveur intermédiaire, à qui l'on devra accorder une grande confiance.

L'*Inria* est l'un des membres fondateurs du projet européen *PEPP-PT* (*Pan European Privacy Preserving Proximity Tracing*). Il vise à proposer des technologies et des standards pour une approche de suivi des contacts fondée sur le consentement, l'anonymat et le respect de la vie privée, en totale conformité avec la réglementation *RDGP*. Vendredi 17 avril, deux établissements suisses, l'*EPFL* (*École polytechnique fédérale de Lausanne*) et l'*EHTZ* (*École polytechnique fédérale de Zurich*), ont choisi de s'écarter du projet. Bien qu'elles soutiennent toujours l'idée d'une collaboration internationale pour mettre en place des solutions de suivi de contacts respectueuses de la vie privée, les deux organisations scientifiques considèrent que le *PEPP-PT* n'est pas assez ouvert et transparent. Même chose pour la *Fondazione ISI*, un institut de recherche italien, ou les Belges de *KU Leuven*, qui ont également décidé de quitter le consortium.

Sans avoir la prétention de recouvrir l'ensemble des controverses ayant trait à cette application, il conviendra ici de s'intéresser aux différents enjeux éthiques que soulèvent les paramètres utilisés pour mener à bien ce projet.

La carte d'identité de StopCovid

Nature des données : données personnelles et de santé.

Stockage :

Lieu : L'application StopCovid fonctionnerait sur une architecture en partie centralisée. En effet, les données seraient alors stockées sur un serveur central, contrôlé par une autorité, mais générées par des terminaux décentralisés, - les smartphones, - qui pourraient communiquer entre eux à travers le *Bluetooth*.

Durée : La durée de conservation n'est à ce jour pas encore définie. Toutefois, Marie-Laure Denis, présidente de la *Cnil*, dans son audition face au Sénat du 15 avril dernier, demandait au gouvernement de rendre l'application « temporaire ». Dans la délibération de la *Cnil* du 24/04/2020 « portant avis sur le projet d'application mobile dénommée « StopCovid » » est précisé que la durée de collecte et du traitement des données générées par l'application sera limitée à celle du l'utilité du dispositif au regard des finalités de l'application.[11]

Anonymisation : Selon l'équipe de l'*Inria* en charge du projet, les données circuleront sous la forme de « crypto-identifiants », c'est-à-dire des données pseudonymisées, généralement générées de manière éphémère (15 minutes) et associées à un terminal et non à un individu. Cependant, les doutes sont nombreux à ce sujet. D'autres chercheurs de l'*Inria* qui étudient les travaux de l'équipe en charge du projet estime que l'anonymisation est impossible. À cet égard, Anne Canteaut, directrice de recherche à l'*Inria*, évoque l'« effet paparazzi »[12] selon lequel tout un chacun pourrait facilement identifier une personne malade du Covid-19. Il suffirait de laisser son téléphone à un endroit pendant une quatorzaine de jours et de s'assurer qu'il n'ait été à proximité que d'une seule personne, pour savoir si cette dernière est atteinte du Covid-19 ou non. *La Quadrature du Net* évoque aussi l'incompatibilité

[11] CNIL. « Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » », *Cnil*, 24/04/2020. Disponible sur <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf>

[12] BONNETAIN, Xavier ; CANTEAU, Anne ; CORTIER, Véronique ; GAUDRY, Pierrick ; HIRSCHI, Lucca ; KREMER, Steve ; LACOUR, Stéphanie ; LEQUESNE, Matthieu ; LEURENT, Gaëtan ; PERRIN, Léo ; SCHROTTENLOHER, André ; THOMÉ, Emmanuel ; VAUDENAY, Serge ; VUILLOT, Christophe. « Le traçage anonyme, dangereux oxymore », *Risques-traçage*, 21/04/2020. Disponible sur <https://risques-tracage.fr/docs/risques-tracage.pdf>

entre l'objectif de l'application - tracer des personnes atteintes du Covid-19 - et la question de l'anonymat. Selon ce collectif, il s'agirait au mieux de pseudonymisation[13].

Technologie : StopCovid reposera sur le *Bluetooth Low Energy*, qui permet un débit du même ordre de grandeur que le *Bluetooth* (1 Mbit/s) mais avec une consommation énergétique 10 fois moindre. Cela permettra ainsi d'intégrer cette technologie dans d'autres équipements tels que les montres connectées, les appareils de surveillance médicale ou encore, des capteurs pour sportifs.

Algorithme : Le logiciel sera libre, en *open source*. Bruno Sportisse justifie ce choix : « *De par son histoire, Inria sait combien le logiciel libre permet à une technologie logicielle d'être améliorée et d'être transparente.* »[14] Cette transparence permet ainsi « *d'apporter toutes les garanties en matière de contrôles par la société : transparence des algorithmes, code ouvert, interopérabilité, auditabilité, sécurité et réversibilité des solutions. Ainsi, cette solution pourrait proposer des briques de base exploitables par tous les pays qui le souhaiteraient.* »[15]

L'utilisation de StopCovid

Finalités recherchées : Dans sa délibération du 24 avril dernier, la *Cnil* précise que la finalité de StopCovid est « *limitée à l'alerte de personnes exposées au risque de contamination* »[16]. Dans un communiqué publié le 4 mai dernier[17], le *Conseil national de l'ordre des médecins* a émis des doutes et a demandé au gouvernement qu'il explicite « *la nature des données que les médecins seront amenés à transmettre* » et la finalité de l'exploitation de ces dernières.

Efficacité incertaine :

Fracture numérique / illectronisme : La condition nécessaire à l'efficacité de StopCovid est son adoption et utilisation massive. Toutefois, comme le mentionne Stéphanie Lacour, spécialiste en droit et innovation au *CNRS* et directrice adjointe des sciences sociales du politique, « *seuls 70% de la population française dispose d'un téléphone qui permet de télécharger l'application* »[18].

Acceptabilité : Une étude réalisée par des chercheurs d'Oxford[19] fin mars a mis en exergue les trois principaux obstacles à l'installation de l'application StopCovid : le risque de piratage de son téléphone (26%) ; la crainte d'un renforcement de la surveillance par le gouvernement après l'épidémie (26%) et la plus grande anxiété que l'utilisation de cette application pourrait susciter (20%). Elle montre aussi que le public français serait autant en faveur d'une installation volontaire que d'une installation automatique (avec possibilité de désinstallation). À Singapour[20], par exemple, l'application TraceTogether n'a été téléchargée que par 1,1 millions de citoyens, soit un cinquième de la population totale alors que le gouvernement indique

[13] La Quadrature du Net. « NOS ARGUMENTS POUR REJETER STOPCOVID », *La Quadrature*, 14/04/2020. Disponible sur <https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/>

[14] Inria. « « Contact tracing » : Bruno Sportisse, PDG d'Inria, donne quelques éléments pour mieux comprendre les enjeux », *Inria*, 18/04/2020. Disponible sur <https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux>

[15] INSERM. « L'équipe-projet StopCovid et l'écosystème des contributeurs se mobilisent pour développer une application mobile de « contact tracing » pour la France. », *Inserm*, 27/04/2020. Disponible sur <https://presse.inserm.fr/lequipe-projet-stopcovid-et-lecosysteme-des-contributeurs-se-mobilisent-pour-developper-une-application-mobile-de-contact-tracing-pour-la-france/39277/>

[16] CNIL. « Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid » », *Cnil*, 24/04/2020. Disponible sur <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf>

[17] Ordre des médecins. « Projet de loi d'urgence sanitaire », *Conseil national de l'Ordre des médecins*, 04/05/2020. Disponible sur <https://www.conseil-national.medecin.fr/publications/communiques-presse/projet-loi-durgence-sanitaire>

[18] BÉCHEREL, Sophie. « StopCovid : le « contact tracing » à la française a-t-il du plomb dans l'aile ? », *France Inter*, 24/04/2020. Disponible sur <https://www.franceinter.fr/sciences/stopcovid-le-contact-tracing-a-la-francaise-a-t-il-du-plomb-dans-l-aile>

[19] ABELER, Johannes ; ALTMANN, Sam ; MILSOM ; Luke ; TOUSSART, Séverine ; ZILLESSEN, Hannah. « Acceptabilité d'une application téléphone pour tracer les contactsporteurs du Covid-19 », 06/04/2020. Disponible sur <https://osf.io/24uan/>

[20] CHONG, Clara. « About 1 million people have downloaded TraceTogether app, but more need to do so for it to be effective: Lawrence Wong », *The Straits Times,* 01/04/2020. Disponible sur <https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for/>

qu'elle serait utile dès lors qu'au moins 75% de la population l'utiliserait. La Belgique a ainsi renoncé à mettre en place une application en citant le cas de l'Autriche, qui ne compte que 3% ou 4% d'utilisateurs.

Ouverture constante de l'application : Lorsque StopCovid est en arrière-plan ou fermée, alors le *Bluetooth* est inactif. L'application doit être en permanence activée pour qu'elle fonctionne. C'est pour cette raison que la réussite de ce projet dépend également d'*Apple* et *Google* qui pourront, *via* leur API, permettre à ceux en charge du développement de StopCovid, permette d'activer le *Bluetooth* en permanence. Cependant, comme l'indiquait Cédric 0 sur *BFM Éco*[21] : « *Apple aurait pu nous aider à faire en sorte que l'application marche encore mieux sur iPhone mais n'a pas voulu le faire, pour une raison que je ne m'explique guère* ». À ce jour, il est ainsi difficile de compter sur eux.

Imprécisions de la technologie *Bluetooth* : La technologie *Bluetooth* n'a pas été conçue pour être précise dans l'estimation de distance entre deux individus. De nombreux paramètres peuvent faire varier les résultats : la physiologie des personnes, la position du smartphone, le type de smartphone, l'état de la batterie, … En réponse à ces limitations technologiques, plusieurs équipes internationales ont mené des tests de calibration pour proposer des modèles statistiques qui tendent à réduire la marge d'erreur.

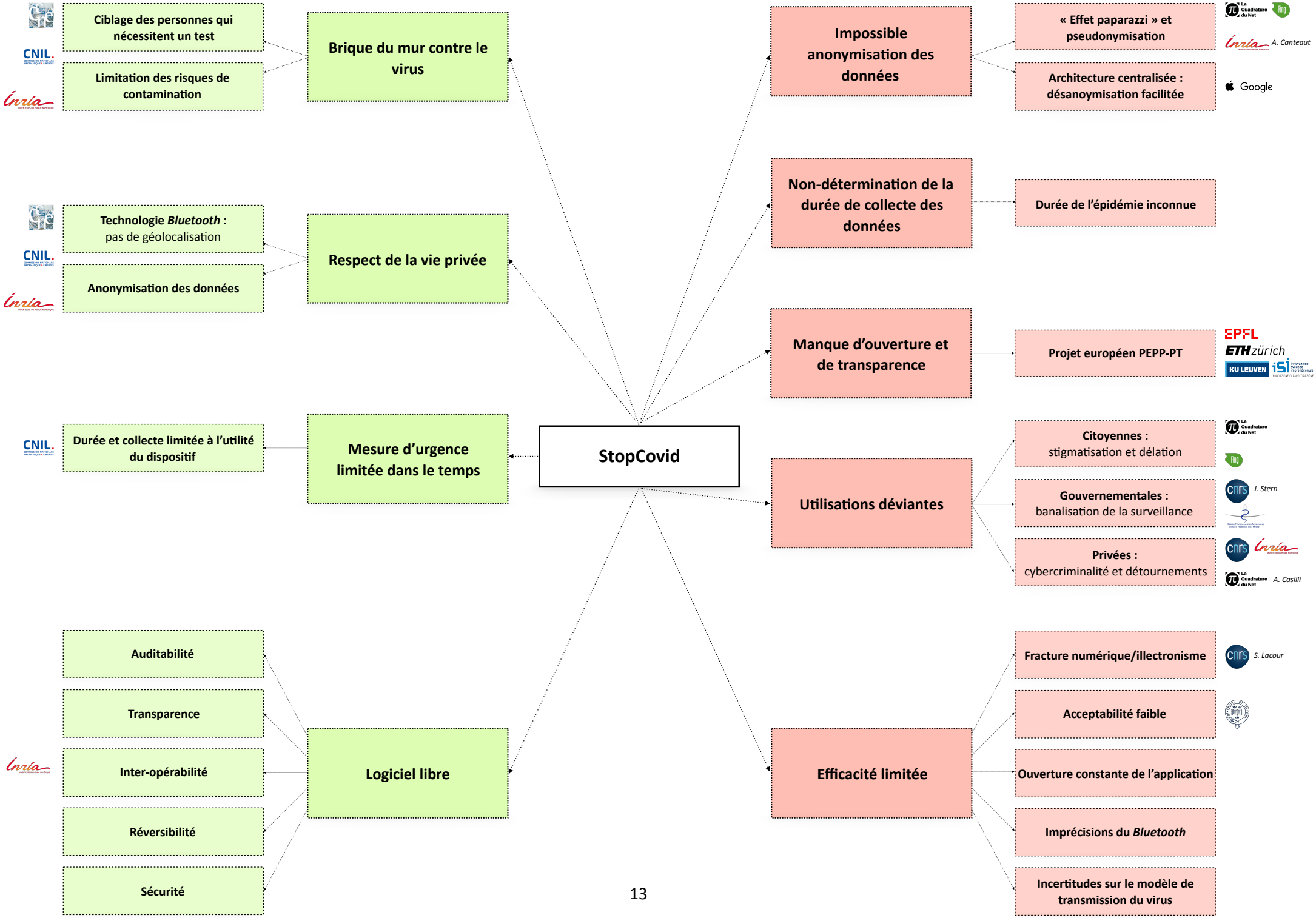
Incertitudes sur le modèle de transmission du virus : l'état de l'art actuel laisse de nombreuses zones d'ombre concernant la manière dont se transmet le virus. C'est autant de paramètres à prendre en compte et qui auront tendance à être modifiés à l'avenir dans le calibrage de l'algorithme (aérosols ou gouttelettes, via les surfaces, charge virale, …).

Risques d'utilisations déviantes : Le risque de l'application StopCovid est qu'elle pourrait encourager la stigmatisation des malades et ainsi, instituer un mode de délation automatique. *La Quadrature du Net* pointe ce risque et imagine une situation[22] dans laquelle l'accès aux tests sérologiques serait favorisé aux utilisateurs de l'application. Par ailleurs, les risques de stigmatisation peuvent être renforcés par l'utilisation de ces applications. Par exemple, en Corée du Sud, suite à de nouvelles contaminations dans des boîtes de nuit homosexuelles, les violences envers la communauté LGBT+ se sont multipliées[23].

[21] BFM Eco. « StopCovid: « Apple aurait pu nous aider à faire en sorte que l'application marche encore mieux sur iPhone mais n'a pas voulu le faire, pour une raison que je ne m'explique guère », 05/05/2020. Disponible sur <https://twitter.com/bfm_eco/status/1257561852885819393>

[22] La Quadrature du Net. « NOS ARGUMENTS POUR REJETER STOPCOVID », *La Quadrature*, 14/04/2020. Disponible sur <https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/>

[23] KIM, Nemo. « More scary than coronavirus South Koreas alerts expose private lives », *The Guardian*, 06/03/2020. Disponible sur <https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives>


StopCovid
Brique du mur contre le virus
Ciblage des personnes qui nécessitent un test
Limitation des risques de contamination
Respect de la vie privée
Technologie Bluetooth : pas de géolocalisation
Anonymisation des données
Mesure d'urgence limitée dans le temps
Durée et collecte limitée à l'utilité du dispositif
Logiciel libre
Auditabilité
Transparence
Inter-opérabilité
Réversibilité
Sécurité
Impossible anonymisation des données
« Effet paparazzi » et pseudonymisation
Architecture centralisée : désanoymisation facilitée
Non-détermination de la durée de collecte des données
Durée de l'épidémie inconnue
Manque d'ouverture et de transparence
Projet européen PEPP-PT
Utilisations déviantes
Citoyennes : stigmatisation et délation
Gouvernementales : banalisation de la surveillance
Privées : cybercriminalité et détournements
Efficacité limitée
Fracture numérique/illectronisme
Acceptabilité faible
Ouverture constante de l'application
Imprécisions du Bluetooth
Incertitudes sur le modèle de transmission du virus

III. Les projections : scénarios possibles pour une application de traçage du Covid-19

Face à ce qui semble être un dilemme cornélien, c'est-à-dire l'impossible choix entre deux valeurs tout aussi importantes, ici la sécurité et la liberté, nous avons décidé d'utiliser une démarche projective. L'objectif final étant de prendre la décision qui maximise les effets positifs et minimise les effets négatifs. C'est, dans une perspective utilitariste, la question du coût d'opportunité : est-ce que le coût en termes de risques pour les libertés fondamentales est inférieur au bénéfice pour la société en matière d'efficacité à stopper l'épidémie Covid-19 (bénéfices sanitaires - éviter des morts -, et socio-économiques - limiter les dégâts potentiellement catastrophiques de cette crise sur les années à venir pour les sociétés -) ?

Nous avons établi les différents scénarios possibles : que se passe-t-il si l'application StopCovid est lancée ? Que se passe-t-il si elle n'est pas lancée ? Que se passe-t-il si l'application qui domine le marché est dirigée par des acteurs privées (Google et Apple notamment) ? Quelles alternatives pouvons-nous proposer ? Ces scénarios sont centrés sur le cas français, ayant ici une valeur d'exemple concernant les enjeux éthiques de cette situation inédite.

Pour chaque scénario, nous appliquerons la doctrine du double effet[24], qui considère que chaque action a à la fois de bonnes et de mauvais conséquences. Il s'agit donc d'observer les conséquences collatérales négatives d'une application de traçage Covid-19. Pour qu'une décision soit prise, il est nécessaire que l'effet positif soit plus fort ou égal au mauvais effet. C'est pourquoi la prise en compte de l'efficacité des applications de traçage est essentielle afin de déterminer s'il est alors acceptable ou non d'assumer les conséquences négatives de ces mêmes outils technologiques.

Le scénario du lancement de l'application StopCovid

Le gouvernement français a fait le choix de lancer l'application StopCovid début juin. Quelle est sa pertinence ? Les débats ont été virulents et les informations ont plusieurs fois évolué.

Les effets positifs

Dans ce scénario, l'application StopCovid serait un outil intégré dans une stratégie globale de lutte contre la propagation du virus. La métaphore de la « brique » pour dresser un mur contre la propagation du virus a été de nombreuses fois convoquée. En effet, certains acteurs craignent que l'application ne détourne les efforts de mesures réellement efficaces comme le port de masques, la distanciation sociale et la réalisation de nombreux tests. Cependant, si un outil est disponible et peut contribuer à mieux optimiser et visualiser la propagation du virus, il semble logique de l'intégrer. L'application StopCovid, en rendant compte des zones de contact, permettrait de cibler les personnes les plus exposées afin de les guider, en incitant par exemple à aller faire un test et à se mettre en quarantaine en cas de résultat positif. Néanmoins, son utilisation à l'échelle nationale n'est possible que si les conditions de respect de la vie privée et du secret médical sont assurées. Pour ce faire, des garanties doivent être prises : le consentement des personnes doit être libre et éclairé, la durée des mesures de suivi doit être fixée jusqu'à une date précise, garantir les conditions de la réversibilité du système - notamment en cas de faille technique -, l'évaluation de la nécessité et de la proportionnalité des mesures régulièrement. Par ailleurs, l'utilisation de cette application est utile pour la recherche en virologie. L'étude des contacts sociaux est une source d'information essentielle pour les épidémiologistes. Des applications peuvent, par exemple, rassembler les données d'hôpitaux et autres établissements de santé. Cette application représente également un avantage de taille pour les ingénieurs qui développent ces systèmes

[24] La doctrine du double effet est théorisée par Saint-Thomas d'Aquin au XIIIème siècle.

numériques afin d'en améliorer l'efficacité et la sécurité. En effet, l'expérimentation d'une utilisation nationale permettrait de réaliser un échantillon de test à grande échelle.

Si l'application s'avère efficace à informer rapidement les personnes à risque, son utilité pour la société serait, évidemment, immense. Nous ne sommes pas compétents pour juger techniquement de l'efficacité de StopCovid, cependant, les avis de spécialistes semblent souvent mitigés : de nombreuses incertitudes ont été soulevées précédemment quant à l'efficacité d'une telle application.

Les craintes et effets négatifs

En considérant les doubles effets négatifs de ce lancement, nous observons un risque majeur : celui d'une banalisation du traçage des populations par l'État. En effet, l'analyse des controverses révèle une cristallisation du débat autour d'une peur : comment se protéger contre les abus des États ? Cette angoisse d'un État liberticide est fondée sur des traumatismes historiques, mais également des exemples de dérives autoritaires actuels. Au premier abord, il semble paradoxal de ne pas accorder de confiance à l'État dans la mesure où le fondement philosophique de ce dernier est une association politique, autrement nommée un contrat ou pacte social[25], ayant pour objectif d'assurer la sécurité des hommes. Cependant, la première moitié du XXème siècle a vu émerger des États totalitaires fondés sur un contrôle et une manipulation de masse des populations. Les grands procès qui ont suivi marquent un tournant dans la conception de l'État : celui-ci est capable de crimes contre l'humanité. Il est donc nécessaire de se protéger contre l'État lorsqu'il s'écarte de sa mission originelle de protection de l'ensemble de ses citoyens.

La généralisation des applications de traçage fait douloureusement écho à l'époque des totalitarismes et effraie par sa puissance technologique bien plus développée que des décennies plus tôt. Par ailleurs, la force symbolique de l'imaginaire qu'elles convoquent contribue à cette méfiance : le traçage des populations est un élément récurrent dans les dystopies technologiques. Méfiance d'autant plus justifiée qu'elle ne se cantonne pas à la science-fiction, mais existe déjà dans certains pays, notamment la Chine. Un récent documentaire réalisé par *Arte*, nommé *Tous surveillés, 7 milliards de suspects*, parle du « premier totalitarisme numérique ». L'État chinois a mis en place un système de « crédit social », attribuant une note à chaque citoyen en fonction de ses actions bonnes ou mauvaises, basé sur une surveillance massive grâce aux outils technologiques. Depuis la pandémie Covid-19, ce système coercitif est devenu encore plus puissant avec l'introduction de données médicales. Par exemple, la température du livreur est affichée en temps réel sur l'application. Si l'application StopCovid est bien loin d'utiliser de tels outils - comme la géolocalisation - et dresse une liste de précautions exhaustives et pertinentes, l'introduction d'un tel outil peut être vue comme un premier pas vers une surveillance de plus en plus importante des populations. C'est d'ailleurs une des raisons pour laquelle l'Allemagne préfère avoir recours à une application développée par les géants privés du numérique que sont *Google* et *Apple* plutôt que de laisser la main à l'État, ayant bien à l'esprit la lourde Histoire de la surveillance de masse sous le régime nazi puis en RDA.

Il convient d'être extrêmement vigilants quant aux conséquences des décisions politiques inédites provoquées par cette crise sanitaire sans éléments de comparaison dans l'Histoire. Lorsqu'il paraissait inconcevable quelques mois plus tôt de confiner un tiers de la population mondiale chez elle pendant deux mois, toutes les pistes, qui s'apparentaient par le passé à de la science-fiction, semblent aujourd'hui possibles. Jusqu'où les États peuvent-ils aller dans la restriction des libertés ? Aux États-Unis par exemple, un pays attaché à la priorité de la liberté sur la sécurité, le confinement provoque déjà de vives oppositions, étant perçu comme une violation des libertés fondamentales - liberté de déplacement et de réunion par exemple -.

Face à ces craintes légitimes, le gouvernement français rétorque que cette solution est absolument temporaire. Un argument qui peine à convaincre puisqu'en 2015, lorsque l'État d'urgence est déclaré en France suite aux attentats djihadistes, le gouvernement prend des mesures restrictives des libertés en assurant qu'elles seront strictement temporaires. Pourtant, cinq ans plus tard, ces mesures d'urgence sont entrées dans le droit

[25] ROUSSEAU, Jean-Jacques. *Du contrat social*, 1762.

commun. Cet exemple récent révèle le processus de banalisation de règles normalement exceptionnelles. Des contraintes auparavant inenvisageables s'installent et sont acceptées par les populations grâce à un climat d'urgence provoqué par un événement soudain. Une fois acceptées, un glissement de la ligne à ne pas franchir s'observe. Cette mesure provisoire peut donc rapidement devenir pérenne. Dans le cas de l'épidémie Covid-19, comment le gouvernement peut-il assurer que l'utilisation d'une application de traçage sera temporaire alors même que la durée de l'épidémie est inconnue ?

Pour éviter une centralisation des informations par l'État, certains acteurs défendent le système *pair-to-pair,* c'est-à-dire que les informations circulent d'un individu à l'autre sans passer pas une instance centralisatrice. Cependant, cette solution présente des risques plus importants concernant la sécurité des données. En effet, les protocoles de traçage décentralisés constituent une liste des personnes atteintes du Covid-19, ce qui peut être extrêmement dangereux en cas de piratage, notamment. Les systèmes centralisés regroupent, quant à eux, un fichier des personnes ayant été en contact avec un malade et donc potentiellement exposées à la maladie. Par conséquent, si la mise en place d'une instance centrale semble plus sécurisée, à qui accorde-t-on confiance quant à la gestion de ces données ? Certains proposent, à l'instar de Tariq Krim[26], que l'ensemble des données soient récupérées par une entité juridique indépendante. Ce système est nommé « fiducie des données » et a pour objectif d'introduire un processus démocratique afin de limiter les potentiels abus de l'intelligence artificielle. Il prend l'exemple de l'application StopCovid : « *si demain, de nouvelles fonctions sont introduites dans l'application, par exemple, un code couleur qui définit si on peut ou pas prendre le métro, ces changements seront débattus par nos élus plutôt que décidés de manière arbitraire par les éditeurs de l'application* ». Sur le long terme, c'est une solution qui semble pertinente puisque les questionnements éthiques au sujet de la gestion des données et de l'intelligence artificielle vont se poser de manière de plus en plus récurrente. La problématique dépasse le strict cadre de la pandémie Covid-19. Il s'agit d'assurer une protection des libertés fondamentales face aux potentiels abus des États ou acteurs privés.

En effet, les acteurs publics ne sont pas les seuls en mesure d'utiliser ces outils à des fins malveillantes. C'est également le cas d'acteurs variés, à titre individuel ou collectif, c'est à dire en allant de votre voisin de pallier à des groupes de cybercriminels. Ces acteurs peuvent se saisir de l'application StopCovid comme d'une opportunité de détourner des informations précieuses.

Les effets détournés

Dans le scénario d'un lancement de l'application StopCovid, les effets détournés de cette dernière sont également un indicateur de prudence important. Quatorze chercheurs français se sont réunis pour rédiger le rapport « Traçage anonyme, dangereux oxymore ; analyse des risques à destination des non spécialistes »[27], dans lequel ils regroupent des scénarios précis d'usages détournés des différentes applications. En effet, il est imprudent de considérer que les comportements des utilisateurs ou acteurs variés suivront des intentions bienveillantes. Dans tous les cas traités, ces comportements déviants conduisent à des risques de discrimination importants. Les chercheurs pointent ici les failles d'un système dont les garanties éthiques peuvent être plus ou moins facilement mises en péril.

Ils pointent notamment du doigt l'impossible anonymisation des données. Dans tous les protocoles étudiés les données sont pseudonymisées, c'est-à-dire que la possibilité de remonter jusqu'au nom de la personne concernée existe. Concrètement, le risque majeur d'un tel système serait de permettre d'établir une liste plus ou moins exhaustive des personnes atteintes du Covid-19. En effet, il est très clairement envisageable

[26] GRALLET, Guillaume. « StopCovid : l'astucieuse alternative que s'interdit la France pour l'instant », *Le Point*, 29/04/2020. Disponible sur <https://www.lepoint.fr/technologie/stop-covid-l-intelligente-piste-que-la-france-s-interdit-pour-l-instant-28-04-2020-2373159_58.php>

[27] BONNETAIN, Xavier ; CANTEAU, Anne ; CORTIER, Véronique ; GAUDRY, Pierrick ; HIRSCHI, Lucca ; KREMER, Steve ; LACOUR, Stéphanie ; LEQUESNE, Matthieu ; LEURENT, Gaëtan ; PERRIN, Léo ; SCHROTTENLOHER, André ; THOMÉ, Emmanuel ; VAUDENAY, Serge ; VUILLOT, Christophe. « Le traçage anonyme, dangereux oxymore », *Risques-traçage*, 21/04/2020. Disponible sur <https://risques-tracage.fr/docs/risques-tracage.pdf>

que les comportements utilisateurs se focalisent sur les interrogations suivantes : comment retrouver qui vous a contaminé ? Comment savoir si une personne précise est ou a été malade ?

Ainsi, si l'application StopCovid ne réalise pas elle-même un fichier des malades, il est possible que d'autres acteurs mettent en place un système parallèle de fichage à grande échelle. Un risque qui se retrouve tant à l'échelle individuelle - avec la mise en place d'une application à contribution collective tel qu'il en existe déjà pour signaler les radars présents sur la route - que collective. Certaines entreprises d'analyse de données sont prêtes à tout pour récolter des informations pertinentes, à l'instar du scandale de *Cambridge Analytica*, et les revendre à des banques ou compagnies d'assurance. De même, le risque de cybercriminalité est bien présent au vue de la multiplication de ces attaques dans les années passées. Les auteurs parlent d'un « *espionnage à la portée de tous* ».

Les implications discriminatoires se dessinent très clairement : suspicion dans le voisinage, discrimination à l'embauche, au prêt bancaire et aux taux proposés par les assurances, disqualifier un adversaire sportif en faisant croire qu'il est malade ou à risque - un faux positif -, etc. Ces comportements de suspicion et de discrimination ont déjà été observés lors du confinement avec des cas d'agressions envers les soignants. Les risques sont donc élevés à court terme, pendant la durée de la crise.

Le scénario du retrait du projet d'application StopCovid

Le fondement théorique du retrait : l'application du principe de précaution

Dans ce deuxième scénario, l'État français refuse finalement de lancer l'application StopCovid en estimant que les risques sont trop élevés au regard de bénéfices trop faibles pour la lutte contre la propagation du virus. En effet, le scénario catastrophe, développé plus haut, dans lequel l'application StopCovid poserait la pierre d'une normalisation du traçage des individus, mais également que soit dressé un fichier parallèle des malades du Covid-19, exige l'application du principe de précaution.

Le principe de précaution stipule que dans « *l'absence de certitudes, compte tenu des connaissances, scientifiques et techniques du moment, ne doit pas retarder l'adoption de mesures effectives et proportionnées visant à prévenir un risque de dommages graves et irréversibles à l'environnement, à un coût économique acceptable.* » C'est un principe d'anticipation des risques qui prône de prendre des mesures de gestion de risques *a priori*, eu égard aux dommages potentiels sur l'environnement et la santé.

Cette recommandation est à la fois défendable du point de vue d'une éthique conséquentialiste et d'une éthique des vertus, développées par Aristote dans l'*Éthique à Nicomaque*. La précaution, dont l'étymologie latine signifie « se tenir sur ses gardes, prendre ses précautions », est la mise en application de la vertue générale de prudence. La vertu de prudence est une disposition de l'esprit dont l'objectif est de délibérer sur ce qu'il convient de faire, en fonction de ce qui est jugé bon ou mauvais. C'est une approche conséquentialiste : « *la réflexion prudente est toujours finalisante, elle connaît les objets en les situant relativement à leur fin* »[28].

Dans la philosophie moderne, le principe de précaution est popularisé par Hans Jonas en 1979 dans son livre *Le principe de responsabilité*. Selon lui, la puissance technologique pose des nouveaux problèmes éthiques. Il soutient que la Terre et ses habitants ne peuvent être l'objet de toutes les expérimentations possibles sur le plan moral. Ce principe a émergé dans les débats liés à la protection du milieu naturel dans lequel l'Humain évolue. Cependant, son application s'étend progressivement vers les domaines de la santé publique et de la sécurité alimentaire.[29]

---

[28] ETIENNE, Jacques. *La prudence selon Aristote*, Revue Théologique de Louvain, 1970, pp. 430-432. Disponible sur <https://www.persee.fr/doc/thlou_0080-2654_1970_num_1_4_1056>

[29] LARRÈRE, Catherine. *Le principe de précaution et ses critiques*, Innovations, 2003, pp. 9-26. Disponible sur <https://www.cairn.info/revue-innovations-2003-2-page-9.htm#no3>

Pendant longtemps, les moyens techniques utilisés par l'Humain afin d'améliorer le bien-vivre étaient considérés comme neutres moralement. Seules les fins visées pouvaient être analysées à l'aune d'une éthique décisionnelle. Cependant, la technologie a, depuis la révolution industrielle, franchi un cap inédit : celui d'un possible effet irréversible sur la nature et sur les conditions de la vie sur Terre. La puissance technique atteinte fait émerger une situation dans laquelle il devient impossible de séparer les effets dommageables des conséquences bénéfiques. Hans Jonas l'explique ainsi dans *La Technique moderne comme sujet de réflexion* : « *l'action a lieu dans un contexte où tout emploi à grande échelle d'une capacité engendre, en dépit de l'intention droite des agents, une série d'effets liée étroitement aux effets 'bénéfiques' immédiats et intentionnés, série qui aboutit, au terme d'un processus cumulatif à des conséquences néfastes dépassant parfois de loin le but recherché* ». Ainsi, l'Histoire l'a tristement montré avec la bombe nucléaire, la technologie peut prendre un tournant inattendu et servir des desseins malveillants.

Dans le cadre des applications de traçage, les craintes des effets négatifs semblent plus fortes que les arguments en défendant les vertus pour la société. Est-ce la ligne à ne pas franchir ? En l'absence de certitudes, il convient ici d'appliquer le principe de précaution. Ce scénario invite à suivre le l'injonction aristotélicienne « *Anankè sténai* », « il faut bien s'arrêter quelque part ».

Les implications politiques d'un tel positionnement

La majorité des pays du monde se penchent sur une application de traçage, prouvant ainsi qu'ils analysent toutes les pistes possibles afin de lutter contre la pandémie. Si certains dénoncent une attitude de « faire semblant d'agir », refuser d'utiliser un outil potentiellement utile que représente l'application StopCovid pourrait se retourner contre l'État dans le cas d'une seconde vague épidémique : pourquoi n'avez-vous rien fait ?

Cependant, un discours politique cohérent peut être développé sur le sujet. La problématique est inédite et impose une décision éthique au regard des valeurs qui fondent notre société. Si, pour le moment, peu de pays se risquent à oser refuser cet outil, la France peut se positionner en leader. Politiquement, utiliser la rhétorique du pays des droits humains avec la fameuse *Déclaration des Droits de l'Homme et du Citoyen*, est un moyen efficace d'emporter l'opinion publique. Un argument d'autant plus défendable que l'Union Européenne est pionnière sur les réflexions de protection des données et de la vie privée, notamment grâce au *RGPD*. De nombreux articles des textes fondamentaux peuvent être cités pour prouver qu'envisager un traçage des populations est une limite à ne jamais franchir, à l'instar de l'article 9 alinéa 1 du *Code civil* dispose que « *chacun a le droit au respect de sa vie privée* ».

D'autant plus que politiquement, cette affirmation permettrait de concrétiser la volonté d'un changement de paradigme fort dû à la crise Covid-19, annoncé à plusieurs reprises dans les allocutions du président Macron. Le 13 avril, il affirme notamment qu'« *il nous faudra bâtir une stratégie où nous retrouverons le temps long, la possibilité de planifier, la sobriété carbone, la prévention, la résilience qui seules peuvent permettre de faire face aux crises à venir* ». Des mots encore vagues mais dont la teneur politique est claire : il faut savoir ralentir l'excès technologique quand il nuit aux droits et aux conditions d'une vie agréable. La prévention appelle, entre autres, à appliquer le principe de précaution quand nécessaire et à la vertu de prudence.

Dans les autres pays, les débats existent également. L'Israël a retiré l'application de traçage qui permettait à la police de vérifier que le confinement était bien respecté, mais conserve l'application de traçage des contacts par géolocalisation. En Espagne, des applications régionales servent simplement à transmettre des informations et aider les personnes qui appellent à évaluer les symptômes, il n'y a donc pas d'application de traçage. En Angleterre et en France, les États développent leur propre application alors que l'Allemagne choisit d'utiliser l'offre du duopole *Google* et *Apple*. La Belgique a, quant à elle, refusé d'utiliser une application de traçage. L'option de ne pas lancer l'application est donc bien possible.

La voie libre à une application contrôlée par *Google* et *Apple*

Si l'application StopCovid n'est pas mise en place ou qu'elle échoue, elle sera inévitablement mise en concurrence avec des applications jugées plus efficaces (mais également plus intrusives), proposées par le secteur privé. *Google* et *Apple* ont annoncé très tôt s'associer pour la première fois de l'Histoire afin de mener un projet d'application dans le but de lutter contre la propagation du virus.

Les effets positifs

L'application proposée par *Google* et *Apple* aura sûrement un avantage technique par rapport à celles développées par les États[30]. En effet, les deux géants américains, qui développent les système *iOS* (*Apple*) et *Android* (*Google*), exigent que le *Bluetooth* ne puisse être utilisé par une application que lorsqu'elle est active et au premier plan ; ce qui signifie que StopCovid ne pourra capter les données *Bluetooth* que si les utilisateurs laissent l'application ouverte, ce qui restreint d'autant plus l'efficacité de l'application. Cependant, *Google* et *Apple* développent leur propre API qui contournera cette règle, ce qui leur conférera un avantage technique de taille. Cette alliance inédite entre les géants américains permet une interopérabilité des systèmes *Android* et *iOS*. De plus, les interfaces utilisateurs seront intuitives, permettant une facilité d'usage qui séduit les utilisateurs. Enfin, les API de *Google* et *Apple* se sont concentrées sur un système qui ne réduit pas l'autonomie des smartphones. Par ailleurs, en ne suivant pas une logique uniquement nationale, l'application renseignera des informations plus complètes. En effet, dans un monde amené à apprendre à vivre avec le virus, l'utilisation d'une application transnationale peut être un avantage non négligeable.

Par ailleurs, l'indépendance de l'application vis-à-vis des États est un aspect rassurant dans certains pays. C'est notamment le cas de l'Allemagne pour les raisons évoquées plus tôt, mais, de manière générale, tous les pays dont la confiance en les instances dirigeantes est faible. Pour certaines populations, la confiance en la bienveillance et les compétences techniques de sécurisation des *GAFAM* est plus forte qu'envers les États. Ces plateformes travaillent depuis des années à l'amélioration de leurs systèmes pour lutter contre la désinformation en ligne. De plus, depuis le début de la crise Covid-19, elles mobilisent leurs efforts pour rediriger les utilisateurs vers les conseils officiels des gouvernements pour que les bonnes pratiques d'hygiène soient mises en avant.

Google et *Apple* ont ainsi annoncé que 22 pays de 5 continents s'apprêtent à utiliser leurs outils, dont certains pays européens. Cette application sera utilisée par les autorités publiques, sauf dérogation autorisant un acteur privé à en faire usage[31]. L'Allemagne opère notamment un revirement de position en adoptant le système américain et non l'application paneuropéenne *PEPP-PT*[32], sur laquelle se base le modèle français.

Les effets négatifs

Mais peut-on réellement faire confiance à *Apple* et *Google* pour stocker et gérer ces données médicales sensibles ? En effet, ces plateformes suivent un objectif avant tout marchand : leur modèle économique est basé sur l'exploitation des données personnelles des utilisateurs afin d'affiner leurs systèmes de recommandations et de publicités ciblées. Comment s'assurer qu'elle ne seront pas utilisées à des fins commerciales ?

---

[30] Le Figaro avec AFP. « Application de traçage : volte-face de Berlin, qui plébiscite Google et Apple », *Le Figaro*, 26/04/2020. Disponible sur <https://www.lefigaro.fr/flash-eco/application-de-tracage-volte-face-de-berlin-qui-plebiscite-google-et-apple-20200426>

[31] ROZIER, Ulrich. « L'outil de Google et Apple entre en action, la France reste isolée en Europe », *Frandroid*, 20/05/2020. Disponible sur <https://www.frandroid.com/marques/google/712626_covid-19-loutil-de-google-et-apple-entre-en-action-la-france-reste-isolee-en-europe>

[32] Le Point. « Application de traçage : l'Allemagne mise finalement sur Apple et Google », *Le Point*, 26/04/2020. Disponible sur <https://www.lepoint.fr/sciences-nature/application-de-tracage-l-allemagne-mise-finalement-sur-apple-et-google-26-04-2020-2372940_1924.php>

L'apparition des applications de traçage du Covid-19 inquiète quant à l'intrusion de certains acteurs dans la vie privée, dans l'intimité de chacun. Cependant, il est légitime de s'interroger : en criant au scandale lorsqu'un État souhaite mettre en place une application de traçage, s'assurant pourtant que les garanties pour la vie privée soient respectées, ne se détourne-t-on pas le débat d'une réalité : les smartphones s'introduisent déjà depuis des années dans la vie privée des individus (géolocalisation, récolte et vente des données, etc), en particulier les *GAFAM*. Pourtant, dans ces systèmes, la notion de consentement est extrêmement large, questionnant le respect de la vie privée, et la méconnaissance des enjeux de protection des données pour les populations est flagrante. Certains se demandent donc : pourquoi tant de bruit au sujet des applications de traçage alors que nous sommes déjà tracés en permanence ?

Le risque ici est de voir se renforcer le pouvoir de *Google* et *Apple.* L'application de traçage leur permettra de traiter de nouvelles données : des données de santé. En Europe, tant les pays que l'Union européenne, peinent à rivaliser et proposer des modèles performants dans le domaine du numérique. Les mêmes risques de sécurité subsistant dans le scénario du privé, *Google* et *Apple* doivent être en mesure de prouver que les données ne seront pas revendues ou révélées. Ils doivent donc faire preuve de transparence.

Les scénarios alternatifs

Quand la controverse se concentre sur le difficile arbitrage entre lancement ou retrait de l'application, public et privé, des solutions alternatives font moins parler d'elles mais n'en sont pas moins pertinentes.

En effet, cette crise est avant tout humaine et le solutionnisme technologique est un écueil dangereux qui détourne l'attention des mesures prioritaires. En effet, l'efficacité de telles applications est remise en cause, notamment à cause de l'incertitude concernant l'acceptabilité et le pourcentage d'utilisation par la population. Nous avons dressé trois scénarios complémentaires faisant office de recommandation. L'idée est de proposer un système hybride qui remettrait de l'humain dans l'information, assurant plus de transparence et de processus démocratique, ainsi que l'exigence d'une coordination européenne.

Le scénario stuff and staff : remettre de l'humain dans l'information

Une mobilisation humaine primordiale

Pour que le virus ne se propage pas, il est primordial que les populations soient formées sur le respect des gestes barrières, la distanciation sociale et les mesures d'hygiène. L'accent doit être mis sur l'accompagnement des personnes en cas de suspicion de Covid-19. Une notification reçue sur une application est-elle suffisante ? Quel sera l'accompagnement fourni aux personnes ne pouvant ou ne voulant se doter de l'application ? Ce scénario envisage un système dans lequel il serait prioritaire de mobiliser de la force humaine, tant dans la prévention que dans la réaction. L'accompagnement sera efficace si les moyens matériels (masques et tests notamment) et humains sont mis à disposition. Cet avis est partagé par l'OMS, qui affirme que « *les applications de traçages ne remplaceront pas l'humain* » et incite à favoriser la télémédecine[33]. De même, pour faire fonctionner une application de traçage, il faut paradoxalement beaucoup d'humains pour qu'elle fonctionne. Une tribune de scientifiques publiée dans Libération appelle à nous armer « d'enquêteurs sanitaires »[34], c'est-à-dire de personnes chargé de remonter les chaînes de transmission du virus. L'Allemagne envisage, par exemple, de recruter 20 000 agents, c'est-à-dire de former cinq enquêteurs pour 20 000 habitants. Ce rôle exige une intelligence émotionnelle et une empathie développer : il s'agit de contacter les

[33] ATS ; EBZ. « Pour l'OMS, les applications de traçage « ne remplaceront pas » l'humain », *RTS*, 06/05/2020. Disponible sur <https://www.rts.ch/info/monde/11304178-pour-l-oms-les-applications-de-tracage-ne-remplaceront-pas-l-humain.html>

[34] SICARD, Didier ; THIEULIN, Benoit ; RONAI, Maurice ; BEAUVALLET, Godefroy ; Pène, Sophie. « Pour faire la guerre au virus, armons numériquement les enquêteurs sanitaires », *Libération*, 26/04/2020. Disponible sur <https://www.liberation.fr/debats/2020/04/26/pour-faire-la-guerre-au-virus-armons-numeriquement-les-enqueteurs-sanitaires_1786298>

personnes atteintes ou à risque, les convaincre de rester en quarantaine, questionner les malades sur des sujets parfois sensibles, etc.

Les outils numériques de soutien à l'action humaine

Le numérique peut aider à former ces enquêteurs, les encadrer et favoriser la coordination en peu de temps, mais il ne peut remplacer la capacité empathique des épidémiologistes et des agents de santé. L'outil numérique peut également servir de relais d'information complémentaire. Il doit proposer un système simple et compréhensible par tous. Par exemple, une application peut sensibiliser sur les bonnes pratiques, afficher les chiffres de taux de circulation du virus et de remplissage des hôpitaux. Elle peut être complétée par un numéro d'appel qui répond aux questions de ceux qui n'ont pas accès à l'application. L'Espagne a, par exemple, mis en place des centres d'appels régionaux dont l'objectif est informationnel. Le contact humain est d'autant plus essentiel que le climat anxiogène provoqué par cette crise sanitaire a des répercussions psychologiques importantes qu'il convient de ne pas laisser de côté. C'est pourquoi les solutions d'information et de télémédecine doivent être mises en priorité. En France, les *Agences régionales de Santé* représentent des relais stratégiques pour remplir ces missions primordiales. Elles sont notamment chargées de répondre aux interrogations de chacun et de guider les personnes présentant des symptômes de la maladie.

Un exemple d'alternative : une application collaborative indiquant le taux de fréquentation d'un lieu public

Enfin, pourquoi ne pas penser une application alternative, reposant sur une logique de groupe et non individuelle ? Par exemple, la mise en place d'une application qui donnerait le niveau de fréquentation des lieux rassemblant beaucoup de personnes, comme les supermarchés, peut guider de manière intelligente les bonnes pratiques des citoyens. Ces applications fonctionneraient sur le système collaboratif, à l'instar des applications qui cartographient les embouteillages de circulation automobile : les utilisateurs signalent eux-mêmes une forte affluence dans un supermarché, ce qui indique donc aux autres consommateurs qu'il serait préférable de venir faire leurs courses plus tard afin de respecter la distanciation sociale. Une solution applicable pour tous les lieux publics comme les parcs, les rues, les plages, etc. L'avantage de cette application est qu'il n'est pas nécessaire que la population entière ait l'application pour qu'elle soit efficace : il suffit que quelques personnes signalent une forte affluence et la zone passe en rouge sur la carte. Elle est basée sur du déclaratif et du *crowdsourcing*, permettant de vérifier la validité d'une déclaration et d'affiner la précision de l'application.

Cette alternative, facile à mettre en place, ne met pas en danger la vie privée car elle considère les risques du point de vue des rassemblements de populations plutôt que sur l'individu, et incite à la responsabilité collective. Elle redonne du pouvoir à l'utilisateur et en appelle au civisme de chacun, ce qui suit non pas une logique d'infantilisation des citoyens de la part des États, mais plutôt de collaboration à l'échelle locale. Enfin, c'est un système qui aide à la prévention des risques et non pas à la détection d'une personne porteuse du Covid-19.

Plus de démocratie et de transparence

Ces problématiques mettent au premier plan du débat un enjeu bien présent depuis des années : quelle protection pour les données personnelles et intime des individus ? La méconnaissance tant des technologies que des enjeux montrent qu'il est nécessaire de faire en sorte que les populations montent en compétence sur ces sujets. Dans ce scénario, il est essentiel de s'appuyer sur le système démocratique afin de contribuer à informer et éduquer aux enjeux numériques, en intégrant davantage la population dans le processus décisionnel. La création d'une commission citoyenne peut, par exemple, être envisagée. Afin d'aller plus loin encore dans cette démarche de transparence et de réflexion, l'enjeu éthique étant de taille, la création d'une entité juridique indépendante, proposée par Tariq Krim et développée précédemment, permettrait de sécuriser la société et les droits fondamentaux des individus face aux potentiels abus des États, acteurs privés ou autre acteurs malveillants, collectifs ou individuels.

C'est, *in fine*, la notion de transparence qui est au cœur de ces démarches. Tout d'abord, la transparence des algorithmes et la compréhensibilité des technologies par les individus. La transparence concerne également les décisions politiques, qui ne peuvent se mener sans l'intégration des citoyens, puisqu'il s'agit, bien souvent, de cas inédits et limites, mettant en cause leurs droits fondamentaux.

Une coordination européenne

Enfin, l'Europe a manqué de coordination et d'une stratégie globale dans le questionnement technologique présent. Bloquée entre des modèles extrêmement coercitifs en Asie et une hégémonie de *Google* et *Apple* du côté outre-atlantique, l'Europe n'a pas de solutions qui soient réellement pertinentes à grande échelle. Dans ce scénario, c'est donc une perspective de plus long terme qu'il convient d'adopter, dépassant le strict cadre du Covid-19. L'espace européen, dont les frontières sont ouvertes à la libre circulation des biens et des personnes, n'a pourtant pas été capable de mettre en place une stratégie globale d'analyse des mouvements de populations en son sein. Pourtant, le scénario d'une Europe coopérative afin d'assurer sa souveraineté numérique permettrait d'atteindre une réelle autonomie politique et technologique. La France a été l'un des premiers pays européens à créer un conseil national du numérique, mais il dépend du gouvernement. Il devient indispensable de créer un institut européen pluripartite portant les enjeux d'éthique des technologies et leurs impacts sur la société au premier plan.

Conclusion

Le Parlement français a validé le lancement de l'application StopCovid le 27 mai 2020. Le gouvernement a insisté sur le respect des garanties suivantes afin de lancer l'application : elle est « *temporaire, d'installation volontaire, non identifiante et transparente* ». Cependant, l'incertitude quant à l'adhésion des citoyens à l'application et donc de son efficacité demeurent. Les opposants au projet craignent une banalisation du traçage des individus et suspectent un recul progressif du respect de la vie privée, sous couvert de crise sanitaire. Tandis que le gouvernement français tente d'assurer la préservation des droits individuels tout en protégeant la population contre le virus, la Chine utilise massivement tous les outils technologiques à sa disposition afin de contrôler sa population, mettant en place le premier totalitarisme numérique d'ampleur du XXIème siècle. Pourtant, alors que la Chine profite de la crise sanitaire pour renforcer la surveillance de sa population, des contestations émergent[35]. En effet, même si la situation sanitaire semble s'être largement améliorée, les responsables politiques annoncent vouloir généraliser les applications de traçage de la santé des individus. A Hangzhou, il est envisagé de mettre en place un classement des citoyens par un *Indice de santé personnel* avec un score allant de 0 à 100 qui prend en compte la durée du sommeil, le nombre de pas effectués, la consommation d'alcool et de tabac, etc. Des citoyens se sont exprimés sur les réseaux sociaux, malgré la répression et les risques majeurs encourus, à l'instar de Wang Xin - 2,5 millions d'abonnés -, qui écrit : « *cela ne viole-t-il pas effrontément la vie privée de surveiller et de discriminer les personnes en mauvaise santé ?* ». Ainsi, la crise du Covid-19 marque un tournant inédit, tant en Europe qu'en Asie, en banalisant l'utilisation massive de technologies de contrôle mais également en plaçant le respect de la vie privée au coeur des enjeux présents et futurs.

[35] ZHONG, Raymond. « China coronavirus surveillance », *New York Times*, 26 mai 2020. Disponible sur <https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html?referringSource=articleShare>