Application #STOPCOVID : Quels impacts sur nos données personnelles ?

Nacira SALVAN
Présidente du CEFCYS

Depuis l'annonce du développement de cette application, beaucoup de questions entourent sa mise en place : Comment ça marche ? Quelles informations personnelles seront utilisées ? Comment seront utilisées les données ? Y a-t-il un risque d'atteinte à la vie privée ? Qui aura accès à ces données ? Les expertes du CEFCYS vous livrent des clés d'analyse (article collectif).

La pandémie de coronavirus a déclenché une crise sanitaire mondiale sans précédent, obligeant toutes les populations à modifier leurs comportements et le gouvernement à opter pour des mesures drastiques de confinement afin de limiter la propagation du virus. Les chercheurs examinent les déplacements des personnes malades pour comprendre comment le coronavirus se propage à très grande vitesse (la chaîne de transmission). Le but est de permettre un déconfinement sans une deuxième vague tant redoutée.

Plusieurs pays, dont la Corée du Sud, Singapour, Taïwan et Israël, se sont tournés vers le digital pour assouplir le déconfinement et tracer la chaîne de transmission. À travers une application, les personnes testées positives au Covid-19 sont identifiées et les personnes qui rentrent en contact avec elles reçoivent une alerte sur leur téléphone.

Dans le même esprit, l'Union européenne a lancé le programme « Pan-European Privacy-Preserving Proximity Tracing » (PEPP-PT). L'objectif affiché est de développer une application de traçage via Bluetooth, avec enregistrement sur la base du volontariat.

Pour la France, l'application se nomme « Stop COVID » et est rentrée en effet le 2 juin avec déjà 1,5 million d'utilisateurs.

Éléments d'analyse

Ce sujet a fait l'objet de nombreuses discussions au sein de notre association, le CEFCYS (Cercle des Femmes dans la Cybersécurité), et nous étions également largement sollicitées par notre entourage. À travers cet article collégial, notre but est de fournir aux lecteurs des informations claires et vérifiées pour soutenir leur décision, et non de prendre parti pour ou contre l'application.

Nous avons fait le choix de rassembler les informations sous la forme d'un SWOT[1], qui est une présentation factuelle.

[1] https://fr.wikipedia.org/wiki/SWOT_(m%C3%A9thode_d%27analyse)

	Positif (Pour atteindre l'objectif)	Négatif (pour atteindre l'objectif)
Origine Interne (Organisationnelle)	**S – Forces** 1. Implications d'entreprises performantes 2. Implication d'institutions reconnues 3. Implémentation de la « Privacy by design » 4. Utilisation d'un traçage de proximité	**W – Faiblesses** 1. Utilisation du protocole Bluetooth 2. Applicabilité de la RGPD (minimisation, anonymisation, limite dans le temps) 3. Publicité pour les partenaires : impact long terme ? 4. Application limitée aux portables
Origine externe (Environnement)	**O – Opportunités** 1. Utilisation du digital pour permettre un déconfinement sans deuxième vague 2. Complément du dispositif par un accès aux tests et aux gestes barrières (masques) 3. Inscription sur la base du volontariat 4. Communication transparente sur la solution mise en œuvre 5. Opportunité européenne sur la RGPD	**T – Menaces** 1. Inscription sur la base du volontariat : difficulté à atteindre le pourcentage requis de participants pour être efficace 2. Volonté des personnes alertées de se faire tester et de se confiner 3. Défiance vis-à-vis du gouvernement 4. Souveraineté numérique 5. Applicabilité de la RGPD (Accès aux données, consentement, sous-traitants, information en cas de fuite) 6. Création d'applications « Pirates » 7. Limitation de l'application à la France

Forces (Strengths)

L'implication d'acteurs majeurs de la Sécurité des Systèmes d'Information (avec notamment l'Inria, ANSSI, Capgemini, Dassault Systèmes, Inserm, Lunabee Studio, Orange, Santé Publique France et Withings) se veut rassurant car c'est l'association d'entreprises performantes et d'institutions reconnues, comme l'Inria qui coordonne le projet. La CNIL[2] a également appuyé ces travaux et est consultée à chaque étape clé du projet.

Il est annoncé que cette application sera respectueuse du RGPD en suivant le principe de « PrivacyByDesign ». « L'application utilisera des pseudonymes et ne permettra pas de remontée de listes de personnes contaminées », explique Marie-Laure Denis, la présidente de la CNIL dans son avis rendu le 24 avril 2020.

Le secrétaire d'État en charge du numérique, Cédric O, sur BFM TV rassure sur les points suivants :

- L'identité de l'utilisateur ne sera jamais dévoilée.
- La collecte, l'identification et la durée de conservation seront limitées.
- La minimisation et dé-identification de l'application sont prônées.

Dès le début, le gouvernement insiste sur le fait que cette application ne sera pas du « tracking », mais un système de « traçage de proximité » et ce « contact tracing » utilisera la technologie « bluetooth » pour être moins intrusive. L'identification sera anonymisée dès la racine de la donnée et sa détention sera éphémère. De plus, le gouvernement a fait le choix de soumettre le code de l'application à des hackers

[2] https://linc.cnil.fr/fr/coronoptiques-34-des-modeles-epidemiologiques-au-contact-tracing-rendre-visible-la-contagion
https://www.cnil.fr/fr/deconfinement-lavis-de-la-cnil-sur-le-projet-de-decret-encadrant-les-systemes-dinformation-mis-en

éthiques, à travers la plateforme de Bug Bounty YESWEHACK.

D'après son article sur l'application, le Journal des femmes indique qu'une fois installée sur le smartphone, l'application préviendra les personnes qui ont été en contact avec un malade testé positif au coronavirus. La personne alertée pourra alors se faire dépister et être prise en charge au plus tôt, ou se confiner afin de briser les chaînes de transmission du virus, même si elle ne développe aucun symptôme. Cette alerte suppose que la personne testée positive au Covid-19 se déclare comme telle et accepte de diffuser cette information aux utilisateurs de l'application qu'elle croiserait dans la rue, les magasins… Cette application sera combinée au répertoire des données.

Deux nouvelles solutions numériques de lutte contre le virus sont en train d'être discutées : Sidep et Contact Covid, qui accompagneront les fameuses « brigades de cas contact » aussi appelées Brigades sanitaires[3].

Faiblesses (Weaknesses)

Tous ces points évoqués sont des forces pour cette application en devenir, mais face à cela de nombreuses faiblesses sont mises en lumière.

Les freins techniques sont pointés du doigt par plusieurs experts en cyber sécurité car la technologie Bluetooth est très critiquée à cause de l'inexactitude des informations Bluetooth et leur qualité.

Au-delà des limites technologiques, il est clair que cette application suscite beaucoup d'interrogations principalement liées à la gestion des données personnelles utilisées et la mise en œuvre réelle des principes de la RGPD :

- Minimisation : est-ce que seules les données nécessaires et suffisantes seront récoltées ? Il y a déjà des exemples en Chine et Corée du Sud de traçage des trajets.
- Anonymisation : l'identité de la personne malade ne doit pas être connue ou induite par les informations disponibles.
- Limitation de conservation dans le temps : Y aura-t-il une transparence sur le cycle de vie intégrale de nos données ?
- Implémentation de toutes les mesures de sécurité informatique nécessaires à la protection de ces données sensibles.

Les entreprises qui participent aux travaux communiquent déjà en disant qu'elles font un geste à titre gracieux, mais l'impact publicitaire est colossal.

Le gouvernement parle déjà d'autres possibilités pour tracer les contacts : boîtier ou bracelet connectés, mais leur élaboration est plus longue et plus coûteuse que l'application pour smartphone.

L'audition de Guillaume Poupard[4] (Directeur de l'ANSSI) est à écouter, car il met en lumière les risques des dérives et d'espionnage, l'impossibilité d'anonymisation totale et les choix politiques d'une telle solution.

Opportunités (Opportunities)

Dans ce contexte de pandémie Covid-19, tous les moyens sont louables pour sortir de cette crise mondiale. L'objectif du développement de l'application a été clairement expliqué par le gouvernement : #STOPCOVID, une application pour smartphone permettra d'aider à limiter la propagation du coronavirus et se fera sur la base du volontariat. Elle sera un complément aux mesures déjà en cours pour munir la population de masques et tester un maximum de personnes pour connaître la sérologie positive ou négative d'un maximum d'individus sur le territoire français.

3 https://www.dataz.fr/

4 http://videos.senat.fr/video.1608918_5ebaa04d6b8cd.audition-de-m-guillaume-poupard-directeur-general-de-l-agence-nationale-de-la-securite-des-systeme

Le Premier ministre ; lors de son audition à l'Assemblée nationale, a insisté sur la nécessité de casser les chaînes de transmission, en identifiant au plus vite les personnes ayant été au contact des personnes infectées. Des brigades sanitaires, d'environ 20 000 à 30 000 personnes, seront chargées de remonter la liste de cas contacts, pour les inviter à se faire tester.

Dans l'article du 6 mai[5], le Secrétaire d'État chargé du Numérique, Cédric O, sur BFMTV le mardi 5 mai, détaillant la feuille de route, assurait que les conditions sont très encadrées et proportionnées. La solution numérique serait même fortement utile selon lui « dans les centres urbains [...], les transports en commun, les lieux publics ou les commerces », où les moyens humains ne permettront pas de reconstituer les chaînes de transmission aussi efficacement que le traitement de données.

L'inscription se fera sur la base du volontariat, il n'y a donc pas d'obligation à l'utiliser.

Les travaux d'élaboration de l'application #STOPCOVID se veulent transparents, le gouvernement communique depuis le début en expliquant qui participera activement au projet. La CNIL a donné son aval et veille au bon déroulé du dispositif en demandant une transparence intégrale au gouvernement, ce qui rassure les experts du RGPD.

Les mesures d'application de ces enquêtes seront précisées par un décret [6]en Conseil d'État, pris après avis de la CNIL, et par ordonnances. L'application de traçage de proximité STOPCOVID pourra être mise en place par ces ordonnances, mais le Premier ministre a promis un débat et un vote spécifique, quand sa mise en œuvre aura avancé.

Pour cela, l'article 6 du décret de la loi soumise, va créer une base de données pour ces enquêtes épidémiologiques. Ce fichier (dont la durée sera de 3 mois, d'après les dernières annonces) pourra contenir des données de santé et d'identification sur les personnes infectées et celles ayant été en contact avec elles, le cas échéant sans leur consentement. Il pourra également être nourri des données de Santé publique France, de l'assurance maladie et des agences régionales de santé. Seuls les services de santé et les laboratoires autorisés à réaliser les tests pourront avoir accès aux données de ce fichier pour les enquêtes épidémiologiques.

Étant donné que les travaux continuent, les informations sont communiquées assez régulièrement et cela montre le bel élan positif ainsi que la force légale du RGPD en France et en Europe. L'opportunité d'harmoniser le RGPD à l'échelle européenne est forte, les pays de l'union ont pu travailler ensemble à travers cet exercice inédit. La tendance du RGPD en France est une valeur indéniable, c'est le « fer de lance » de la France d'après le commissaire européen Thierry Breton, chargé de la politique industrielle, du marché intérieur, du numérique, de la défense et de l'espace. L'objectif est de mener à bien ce projet d'utilité publique pour sortir de la crise sanitaire.

Menaces (Threats)

Cette influence positive du RGPD est souvent éclipsée par les menaces immédiates perçues par la population française, les détracteurs ne manquent pas de souligner les nuisances d'une telle application, les mauvais exemples dans certains pays étrangers et les obstacles à son bon fonctionnement.

La première menace à la bonne efficacité de l'application est l'inscription sur la base du volontariat : le volontariat doit être de minimum 60 % de la population pour faire reculer la maladie Covid-19. De plus, les personnes ayant été malades doivent s'identifier comme telles et avoir confiance dans le système pour fournir cette information.

Ensuite, il est impératif que les personnes qui reçoivent une alerte suivent le protocole, se fassent tester et se confinent. Si ce protocole n'est pas suivi, le virus continuera de se propager.

[5] https://www.linternaute.com/

[6] Dalloz actualité, 29 avr. 2020, art. P. Januel

Malgré les garanties apportées pour minimiser les risques sur la vie privée et les libertés individuelles, persiste le caractère menaçant des moyens technologiques assimilés, par une frange de la population, à des procédés de suivi de masse. L'application fait débat et les détracteurs ne manquent pas de souligner le caractère liberticide d'une telle application. Ainsi, en fonction du degré de confiance en notre système démocratique, déjà secoué par des vents contestataires depuis plusieurs années, l'application peut être perçue comme les prémisses de dérives totalitaires.

Loin des enjeux géopolitiques visant à maintenir une souveraineté numérique face aux acteurs privés disposant de moyens technologiques équivalents - GAFAM, cette défiance vis-à-vis de l'autorité publique se fait omniprésente alors même que l'usage de ces mêmes moyens par ces firmes privées suscitent une adhésion quasi généralisée depuis plusieurs années. Les données personnelles et la vie privée pourraient donc être détenues par des firmes privées sans que cela ne soit perçu comme un risque majeur par les individus alors même qu'une application visant à juguler les risques de propagation d'un virus mortel suscite une levée de boucliers.

La réelle application de la RGPD est au cœur de nombreuses craintes :

- Nous sommes en droit de nous demander où iront nos données ? De plus, les risques de perte et de fuite ne sont pas faibles, quelles seront les conséquences, les dommages et les accès inappropriés ?
- Au-delà d'un usage et une exploitation commerciale non souhaités de ces données, nous ne sommes pas à l'abri d'une exploitation malveillante, est-ce que les mesures de protections et de sécurité sont correctement implémentées ?
- Les exigences métiers sont-elles respectées pour toute personne ayant accès à ces données ?
- La politique de contrôle n'est-elle pas ambigüe au vu du contexte de pandémie (exemple : inscription des utilisateurs parfois compromis avec une violation de l'inscription) ? Les restrictions et les mécanismes sont-ils respectueux en termes de limitation et d'accord ? Les sous-traitants pourraient éventuellement faire fuiter des DCP sensibles avec une grande pluralité des acteurs, seront-ils tous bien identifiés ?
- Quid du Fichier de collecte de données de santé : l'assurance maladie recense déjà nos données de santé et le fichier est créé par ce biais, mais qui d'autre pourra accéder à ces informations ? (politique de développement sécurisé, protection des données de test, visibilité dans un volet du Dossier Médical Partagé en ligne?)
- En cas de violation des données à caractère personnel sensibles, y aura-t-il un bon suivi : enregistrement des incidents ?
- Nous sommes en droit de nous demander s'il sera vraiment possible de retirer son consentement comme l'exige le RGPD : si on télécharge l'application, peut-on tout de même s'opposer au traitement de nos données ? Pourra-t-on se rétracter, et sous quel délai ? (Quid d'une demande légitime de Demande D'accès Aux Données Nominatives Collectées).
- Quelles sont les mesures de transmissions des Données à Caractère Personnel (fuites vers d'autres pays, attention au transfert entre juridictions) Comment pouvons-nous garantir que les données de santé d'une personne contaminée puissent transiter en toute sécurité vers un système standardisé équivalent au notre, au sein de la zone Europe ?

La question de la souveraineté numérique se pose également. Où seront hébergées ces données ? Pouvons-nous avoir confiance alors que tant de données sensibles seront en jeu ? Certains pays (hors UE) sont moins scrupuleux à l'utilisation des données personnelles et de grosses dérives de surveillance de masse sont craintes[7].

[7] https://www.lemonde.fr/idees/article/2020/05/14/l-europe-doit-tracer-le-covid-19-sans-les-gafam_6039656_3232.html
https://www.zdnet.fr/blogs/50-nuances-d-internet/la-vie-privee-ou-la-sante-telle-n-est-pas-la-question-39903763.htm

Les acteurs privés et les puissances étrangères n'ont pas attendu pour déployer des arsenaux technologiques qui risquent d'impacter, à terme, notre souveraineté numérique.

Pire, de nombreux Français ont déjà téléchargé une application développée par la Géorgie : de nombreuses applications « Copycat » fleurissent et n'offrent aucune garantie sur la protection des données ou la réelle efficacité de l'application. Le risque est grand pour un usager de télécharger la mauvaise application.

Pour le moment, l'application sera faite pour la France, ce qui ne répond pas au besoin de nombreux frontaliers. Chaque pays de l'UE est en train de développer et tester sa propre application et ne prend donc pas encore en considération les personnes qui dans le cadre de leur travail effectuent quotidiennement des trajets hors France.

Pistes d'amélioration

Plusieurs pistes d'amélioration sont possibles pour permettre un plein succès de l'application STOPCOVID :

1. Renforcement du Bluetooth par le protocole ROBERT. Pour être crédible au niveau européen le consortium PEPP-PT (Pan-European Privacy Preserving Proximity Tracing) a créé le protocole ROBERT[8]. L'inria en France et Frauhofer en Allemagne sont à l'origine de ce protocole pour équiper plusieurs pays du continent.
2. Certification ISO27701 de l'application pour garantir une mise en œuvre totale et transparente du RGPD au sein de l'application.
3. Mise en place d'une application unique à l'échelle européenne pour répondre au besoin des frontaliers, et montrer un succès européen dans la gestion de cette crise sanitaire.
4. Création de bracelets ou autres objets connectés pour ouvrir l'utilisation de l'application aux seniors, les plus sensibles au virus, mais les moins équipés en téléphone portable.

L'influence de l'ISO 27701 tombe à point nommé, car cette norme internationale reflète les exigences RGPD, le code de bonne pratique et le cadre de la protection de la vie privée. Ce cadre permet de mieux comprendre dans quelles mesures nos données personnelles peuvent être collectées de manière respectueuse. L'objectif est d'atténuer les risques de ce traitement massif de données en prouvant la transparence à travers des informations claires, précises, simples et concises pour le public ciblé.

Parmi les exigences de l'ISO27701, notons les points suivants :

- Protection des Données externes à caractère personnel : l'entreprise doit documenter tout stockage de Données à Caractère Personnel (supports/dispositifs/chiffrement/procédures/mesures compensatoires).
- PIMS RGPD (Système de gestion des données personnelles) : clarifient les exigences liées aux Sous-Traitants et aux Responsables de Traitement.
- La Sécurité physique et environnementale doit être assurée : zone, emplacement, protection, sorties des actifs, procédures, gestion des changements, sauvegarde des informations.

Cette application fait partie d'un ensemble de mesures qui permettra de reprendre l'activité économique rapidement et en toute sécurité. L'application n'est qu'un maillon de la chaine de protection. L'humain et sa santé sont des priorités qu'il faut pérenniser et protéger.

Le sujet de l'application STOPCOVID est particulièrement épineux dans la mesure où il pose le

DCP : Données à Caractère Personnel

[8] https://siecledigital.fr/
PROTOCOLE ROBERT pour Robust and privacy-presERving proximity Tracing protocol

débat de la proportionnalité des moyens nécessaires à la maitrise de risques de surmortalité liés à la pandémie actuelle. Qui dit situation exceptionnelle, dit moyens exceptionnels.

Les démocraties sont-elles prêtes à accueillir, sans renier leurs principes fondamentaux, les nouvelles vagues technologiques qui fournissent des moyens de plus en plus puissants pour collecter et traiter les données des populations ? C'est tout l'enjeu politique autour de l'application STOPCOVID.