Analyse d'impact pour une application aidant à la lutte contre la propagation du COVID-19

Kirsten Bock
kirsten.bock@fiff.de

Christian Ricardo Kühne
demian@fiff.de

Rainer Mühlhoff
rainer.muehlhoff@fiff.de

Měto R. Ost
meto.ost@fiff.de

Jörg Pohle
joerg.pohle@fiff.de

Rainer Rehak
rainer.rehak@fiff.de

Version 1.2 – 24 avril 2020

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V.

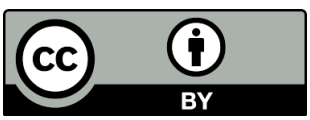
Contact : dsfa-corona@fiff.de

https://www.fiff.de/dsfa-corona

https://www.fiff.de/dsfa-corona

Version 1.2 (FR) published 24 avril 2020.
Version 1.0 (DE) published April 20, 2020.

Document available here :
https://www.fiff.de/dsfa-corona



Résumé et résultats de l'analyse

Depuis que le coronavirus s'est étendu à l'Europe début 2020, il est devenu nécessaire d'associer une vision technique aux débats publics et politiques : la pandémie pourrait éventuellement être endiguée par la mise en place d'applications mobiles de suivi. Ces systèmes auraient vocation, de manière automatique, à référencer les interactions entre utilisateurs et permettrait ainsi d'obtenir, rapidement et efficacement, une représentation de la chaîne d'infection et d'isoler les personnes exposées au virus dans les meilleurs délais.

Des États comme Singapour, la Corée du Sud ou Israël ont choisi de mettre en place des solutions plus radicales, incompatibles avec les systèmes juridiques européens car représentatives de limitations déraisonnables à nos libertés fondamentales. En réaction, des initiatives européennes ont vu le jour : en particulier, le consortium *Pan-European Privacy Preserving Proximity Tracing* (PEPP-PT), qui, travaillant à un projet d'application de suivi dans le cadre de la propagation du coronavirus, tient compte des obligations liées à la protection des données – ou, tout du moins, à la privacy, ces deux termes n'étant pas synonymes. C'est ainsi que des systèmes de suivi, comparables à ceux d'autres pays situés hors-Europe, sont conçus de manière plus respectueuse des principes de protection des données. Depuis plusieurs semaines, le discours des médias entend promouvoir cette idée : les applications contre le coronavirus *made* in Europa promettent de garantir le respect de la vie privée des utilisateurs et d'être conformes au Règlement général sur la protection des données (RGPD).

Pour autant, la protection des données à caractère personnel ne saurait être une simple question à laquelle on peut répondre oui ou non : il s'agit d'une mise en balance complexe qui nécessite une discussion précise et détaillée. Le RGPD impose aux responsables de traitement de données (une application de suivi devrait être considéré comme un traitement – voir chapitre 6) de réaliser une **analyse d'impact relative à la protection des données** (PIA) lorsque ce traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes. Une telle analyse correspond à une analyse de risques structurée qui vise à identifier et à évaluer, en amont, les conséquences sur la protection des données.

Les systèmes de suivi dans le cadre de la lutte contre la propagation du coronavirus représentent une expérience sociétale de suivi comportemental numérique sous contrôle étatique en Europe. L'efficacité et les conséquences de ces applications ne sont pas encore connues et il est prévisible que différentes variantes, selon les pays européens, soient testées et évaluées. Les conséquences relatives à la protection de la vie privée et des libertés fondamentales de cette initiative ne toucheront pas uniquement l'individu mais la société dans son ensemble. Dans cette optique, une analyse d'impact ne doit pas seulement être réalisée mais doit faire l'objet d'une publication et d'une discussion publique. Du fait qu'aucun des acteurs concernés n'a présenté ni rendu accessible une telle analyse d'impact et que les privacy impact assessments disponibles ne sont pas complètes, nous – un groupe de scientifiques et d'experts en matière de protection des données dans le cadre du *Forum InformatikerInnen für Frieden und gesellschaftliche Veranwortung (FIfF) e.V.* - avons, de notre propre initative, réalisé une telle analyse d'impact qui se veut une contribution constructive au débat.

Procédure appliquée

Pour la réalisation de cette analyse d'impact, nous nous fondons sur les concept-cadres (appelés frameworks) et projets d'application développés au niveau européen utilisant la technologie de la détection proche au moyen du Bluetooth Low Energy (BTLE).Pour la réalisation de cette analyse d'impact, nous nous fondons sur les concept-cadres (appelés frameworks) et projets d'application développés au niveau européen utilisant la technologie de la détection proche au moyen du Bluetooth Low Energy (BTLE). Ces initiatives sont portées, entre autres, par le PEPP-PT [1], par le DP-3T [2] et par Linus Neumann, membre du CCC, qui a résumé un concept plus général [3]. Le PEPP-PT propose un concept-cadre, c'est-à-dire des spécifications pour un tel traitement par voie applicative plutôt qu'une application à proprement parler. Dans ce cadre, plusieurs implémentations (systèmes / applications) sont envisageables pour mettre en place le framework (le projet DP-3T est une proposition concrète). Le framework proposé par le PEPP-PT laisse la liberté à chaque État européen de développer sa propre implémentation. L'objectif est de permettre, d'une part, une liberté de conception et de prévoir, d'autre part, une interopérabilité au-delà des frontières.

Ainsi, et c'est l'une des conclusions centrales de notre évaluation, les frameworks considérés – et en particulier celui du PEPP-PT – **laissent le choix concernant des caractéristiques et paramètres qui sont directement liés à des questions relatives à la protection des données**. De manière schématique, il existe trois architectures qui sont compatibles avec le cadre proposé par le PEPP-PT (voir chapitre 1) :

a) une **architecture centralisée** : l'anonymat des utilisateurs et la confidentialité de leurs interactions ne valent que pour les tiers (autre utilisateur ou acteurs externes) ; les responsables de l'application et les autorités compétentes peuvent identifier les utilisateurs et les associer à leur historique d'interactions.

b) une **architecture partiellement décentralisée** qui permet également une **recherche épidémiologique** (DP-3T) : les données des utilisateurs et celles relatives aux prises de contact ne sont confidentielles que vis-à-vis des tiers (autre utilisateur ou acteurs externes). Le serveur a la possibilité de désanonymiser les utilisateurs infectés. L'application a une fonctionnalité de « don de données » par laquelle un utilisateur donne accès à son historique d'interactions pour les recherches médicales. Dans ce cas, les interactions des personnes contaminées sont également accessibles aux responsables de l'application et aux autorités compétentes.

c) une **architecture complètement décentralisée** (voir Neumann 2020) : les utilisateurs restent anonymes entre eux et les données relatives à leurs interactions sont confidentielles. Les responsables de l'application et les autorités compétentes ne peuvent désanonymiser que les utilisateurs contaminés et pas leur historique d'interactions. Les données ne peuvent être réutilisées à des fins de recherches médicales.

1. Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) (2020). url : `https://www.pepp-pt.org/` (visité le 08/04/2020)

2. Carmela Troncoso et al. (2020). *Decentralized Privacy-Preserving Proximity Tracing*. White Paper Version : 10th April 2020

3. Linus Neumann (2020). *« Corona-Apps » : Sinn und Unsinn von Tracking*. url : `https://linus-neumann.de/2020/03/corona-apps-sinn-und-unsinn-von-tracking/` (visité le 09/04/2020)

Les responsables de l'application et les autorités compétentes peuvent...	Hypothèse a	Hypothèse b	Hypothèse c
... Les responsables de l'application et les autorités compétentes peuvent	Oui	Non	Non
... Désanonymiser les utilisateurs contaminés	Oui	Oui	Oui
... Désanonymiser les utilisateurs contaminés	Oui	Partiellement	Non

Notre **analyse d'impact porte essentiellement sur l'hypothèse c qui nous paraît plus respectueuse des principes relatifs à la protection des données à caractère personnel**. Nous évoquons également certaines points techniques relatifs à l'hypothèse b.

Les conclusions montrent, en premier lieu, que **même avec une architecture décentralisée, il existe des faiblesses** (voir chapitre 7) **et des risques graves** auxquels il faut remédier. En second lieu, lorsque des comparaisons entre les hypothèses de centralisation ou décentralisation sont faites, elles indiquent que **le choix entre ces deux architectures a de réelles incidences en matière de protection de la vie privée**. Il n'est donc pas possible de conclure qu'une implémentation en accord avec les principes du concept-cadre proposé par le PEPP-PT respecte nécessairement la vie privée.

Points importants, risques et solutions proposées

Nous reprenons ici une sélection des principaux points, risques et solutions proposées :

1. Les discussions actuelles font souvent état du choix laissé à l'individu d'utiliser ou non l'application. **Cette liberté est une illusion.** Il est possible, et cela fait déjà l'objet de certaines discussions, que l'utilisation de l'application soit une condition permettant l'assouplissement des mesures de confinement. La présentation de l'application pourrait permettre l'accès à des bâtiments publics ou privés, à certains espaces ou à des évènements. Il est pensable que les employeurs s'adapteront bien vite à ces mesures dérogatoires ; ils pourront ainsi, à l'aide de mesures prises volontairement, reprendre plus rapidement leur activité. Ce scénario signifie une incitation implicite à l'utilisation de l'application et impliquera vraisemblablement une différence de traitement au détriment des non-utilisateurs. Chaque personne n'ayant pas nécessairement de téléphone, il s'agirait en outre d'une discrimination envers un groupe déjà défavorisé.
2. **La protection des libertés fondamentales sera mise à mal sans pondération et définition de finalités précises.** Il existe un risque élevé concernant l'enregistrement de fausses expositions pouvant engendrer une mise en quarantaine pour l'individu (par exemple : enregistrement d'une interaction à travers un mur séparant deux logements). Afin de répondre à ce risque, il faudrait mettre en place une fonctionnalité permettant à l'utilisateur de pondérer les données de l'application. Ainsi, pourraient être prévues : la révocation de fausses déclarations de contamination, la suppression de fausses interactions avec une personne infectée ou la contestation des mesures restrictives prises sur la base du traitement. Cette possibilité n'est encore prévue par aucune des applications.

3. **Tous les types de traitements évoqués traitent des données de santé.** Le traitement est constitué par le traitement des données de contact enregistrées sur le téléphone, le transfert de ces données sur un serveur après qu'une contamination ait été diagnostiquée puis leur transmission à tous les téléphones permettant de déterminer l'existence ou non d'une interaction avec une personne contaminée. Toutes les données sur un téléphone doivent être considérées comme des données à caractère personnel et notamment comme se rapportant à l'utilisateur de l'appareil. Seules les personnes diagnostiquées comme positives au coronavirus voient leurs données transférées, ces données deviennent ainsi des données de santé. De telles données font l'objet d'une protection au titre du RGPD.
4. **L'anonymat des utilisateurs doit être garanti par le biais de mesures juridiques, techniques et également organisationnelles.** Seule une approche pluridimensionnelle garantira la séparation entre les données traitées et l'identification de la personne efficacement et de manière irréversible afin que l'on puisse parler de données anonymisées. Toutes les propositions actuelles ont pour point commun de ne pas présenter de manière explicite un tel procédé de séparation. Nous avons formulé dans cette analyse d'impact des exigences juridiques, techniques et organisationnelles dont l'implémentation permettra dans la pratique une séparation efficace et irréversible. C'est seulement à cette condition que les données des personnes infectées, sans que celles-ci ne soient identifiées ni identifiables, devraient être sauvegardées sur un serveur et être transmises aux applications de suivi.

Pour une présentation exhaustive des risques et faiblesses, nous vous invitons à vous reporter au chapitre 7 et pour les mesures de protection au chapitre 8.

Généralement, selon la logique de la protection des données, **les risques du traitement mis en œuvre qui émanent principalement du responsable du traitement.** Il est alors nécessaire d'empêcher les usages abusifs du traitement, notamment pour éviter que le traitement n'excède sa finalité, par le biais de mesures juridiques, techniques et organisationnelles. Les promesses des responsables des traitements de respecter la réglementation applicable ne sont pas suffisantes. Les mesures prises doivent pouvoir être contrôlables et faire l'objet d'une documentation.

Le développement en *open source* des applications, par exemple sous le format de logiciels libres, est une condition importante contribuant à la **transparence relative au respect des principes de la protection des données**, non pas seulement à l'égard des autorités de contrôles en matière de protection des données mais également à l'égard des personnes concernées et de la société (civile). C'est seulement ainsi qu'il sera possible de faire naître la confiance de tous, même de ceux qui ne comprennent pas tous les détails techniques.

Les tiers sont également un facteur de risques pour les libertés individuelles. Il ne faut pas penser en premier lieu à des hackers mais plutôt à des **acteurs commerciaux** comme par exemple des responsables de grandes plateformes, et aux acteurs étatiques. Le cas échéant, ces acteurs peuvent bénéficier de meilleurs revenus grâce aux données de suivi qu'ils pourront évaluer eux-mêmes du fait que le Bluetooth soit activé en permanence pour l'application de suivi contre le coronavirus ou en ayant accès aux données sauvegardées chez des acteurs privés.

Les analyses doivent porter sur l'ensemble du traitement de données et non pas uniquement sur les traitements réalisés par les applications. Dans le débat public et pour les différents projets d'application, sont évoquées la protection de la sphère privée, c'est-à-dire la confidentialité à l'égard des responsables de traitement

et des tiers, et la sécurité informatique comme les mesures de chiffrement. A notre sens, cette vision réductrice du sujet évince d'autres risques fondamentaux comme les risques d'ordre politique ou sociétal. Nous avons choisi de les inclure à notre analyse car ils doivent être pris en compte, au risque, sinon, d'être occultés dans le débat public.