l'application Corona "volontaire“

[Partout en Europe se multiplient les initiatives pour implémenter une application, dite de “traçage” qui se veut en accord avec les “démocraties libérales européennes”. Derrière le nom StopCovid en France se cache le même modèle de potentielle surveillance de masse qu’ailleurs. Dans le but d’éclaircir la discussion sur le sujet dans le milieu militant français, nous avons traduit la présentation de l’appli allemande et son analyse par le collectif allemand capulcu (capulcu.blackblogs.org), ndlt.]

En vue d\'une sortie progressive des limitations de contact dans le cadre du Coronavirus, le gouvernement [allemand] mise sur une large acceptation d’une application, téléchargeable après Pâques, pour la reconstruction a posteriori des contacts des contaminés. La peur (légitime) du virus est utilisée pour faire avaler “volontairement” à une majorité de la population un outil autoritaire très efficace. Dans cet article, nous critiquons la construction technique de cette application, mais aussi ses conséquences social-technocratiques. Quand bien même le listage des contacts s’effectuerait totalement sous pseudonyme, nous devons urgemment dénoncer cette application. Dès le moment où des données de comportement (même anonymes) sont collectées à grande échelle, alors les modèles de prédiction qui sont ainsi entraînés sont en mesure de catégoriser toute la population en groupes de risques et à la gérer par algorithmes. A cela s’ajoute qu’une simple actualisation de l’application (software update) la transforme en un outil efficace pour les limitations individuelles d’accès [aux espaces publics et services. Donc : un “non” clair et net pour la Corona-App !

Une équipe internationale composée d’environ 130 scientifiques, développeuses.rs en Technologies de l\'Information et de la Communication (TIC; angl. IT) chargé.es de la protection des données, et soldat.es, travaille actuellement sur un projet du nom de Pan European Privacy-Protecting Proximity Tracing (PEPP-PT) pour un logiciel qui serait censé limiter la propagation du virus SARS-CoV-2. Du côté allemand y participent l’Institut Robert-Koch (RKI), l’Institut Heinrich-Herz (HHI) et l\'office fédéral de la sécurité et de la technique d’information (all. BSI : Bundesamt für Sicherheit in der Informationstechnik). Le chargé fédéral de la protection des données accompagne lui aussi ce développement et des soldat.es de la Bundeswehr participent aux tests. En dehors du RKI, aucun des participants nommés ci-dessus n’est listé sur le site internet du projet [le RKI est justement un conseiller du gouvernement allemand, ndlt]. Le HHI est subordonné au Fraunhofer. Pour l’instant participent au développement des chercheuses.rs et instituts de huit pays: l’Allemagne, l’Autriche, la Belgique, le Danemark, l’Espagne, la France, l’Italie, et la Suisse.

Pour ralentir la propagation, on suppose que les personnes ayant été en contact avec les contaminé.es devraient être averties tôt. Quand les contaminé.es montrent des symptômes, alors iels ont d’ores et déjà contaminé d’autres personnes. C’est pourquoi tou.tes les propriétaires de portables ayant été dans les parages de la personne malade sont censé.es recevoir une notification après un résultat positif au dépistage de ladite personne. Si se multiplient des initiatives isolées et des solutions de logiciels de ce type que seulement une petite partie de la population utiliserait, alors le concept ne peut pas fonctionner. C’est pourquoi il est censé y avoir une base commune, qui puisse atteindre le plus vite possible une taille critique. Il est question d’une plateforme commune : une implémentation de référence client/serveur, mais on parle aussi d’un squelette de logiciel qui puisse être adapté en application de smartphone [comme par exemple l’appli StopCovid en France, ndlt]. Ces applications de smartphone que les utilisateurs.trices installent sur leurs téléphones constituent une partie considérable du système.

En Allemagne, RKI et HHI travaillent à une telle utilisation. Pour pouvoir briser une chaîne d’infection avec efficacité, les chercheuses.rs visent une base d’utilisateurs.trices d’environ 60% de la population. Dans le cas de l’Allemagne, ce serait 50 millions de personnes. Jusqu’à aujourd’hui, en Allemagne, encore aucune application qui ne soit pas préinstallée sur le smartphone et doive donc être téléchargée consciemment, n’a autant d’utilisateurs/rices. Par ailleurs, un nombre d’utilisateurs.trices moindre pourrait déjà aider à au moins ralentir la propagation. Selon Bitkom, 81% de toutes les personnes de plus de 14 ans en Allemagne possèdent un Smartphone. Les portables normaux et les appareils plus anciens ne supportent pas encore le standard Bluetooth nécessaire. Les seniors en particulier, pour qui le virus est particulièrement dangereux, ne pourraient être qu’en partie averti.es. Par conséquent, les chercheu.rs/ses réfléchissent à distribuer prochainement des bracelets Bluetooth ou autres Wearables. Selon un sondage représentatif (au 31/03/2020), plus de 70% des personnes interrogées téléchargeraient une telle application à coup sûr ou bien l’utiliseraient probablement. La plupart des interrogé.es dit vouloir suivre les recommandations de l’application et se mettre en quarantaine dans le cas où iels auraient été en contact avec une personne contaminée. Selon des sondages, une majorité de la population de

l’Allemagne serait prête à abandonner un pan de sa sphère privée pour stopper le virus. La plateforme PEPP-PT devrait être fin prête le 7 avril.

Le RKI et le HHI veulent publier l\'application environ une semaine après pour les utilisateurs.trices allemand.es. Ce système se veut une contre-proposition face aux approches répressives et invasives des autres pays. Au lieu d’accumuler massivement des données de géolocalisation, de surveiller les utilisateurs.trices ou de coller les contaminé.es au piloris digital du Corona, le PEPP-PT se veut complètement volontaire et respectueux de la protection des données. Les exploitant.es promettent de protéger la sphère privée des utilisateurs.trices du logiciel. L’identité des utilisateurs.trices reste confidentielle à tout moment, disent-ils : ni les médecins, ni les exploitant.es de la plateforme ne peuvent identifier les individus. Les journaux s’occupent de faire de la bonne publicité en parlant même d’une utilisation “anonyme”, alors qu’il s’agit en fait d’une mise sous pseudo. Le modèle PEPP-PT ne paraît pas non plus respecter ni viser les 100% au Privacy-by-Design [« protection de la vie privée dès la conception », ndlt]. Les spécifications et le code source ne sont pour l’instant fournis, selon le site internet - jusqu’ici très pauvre en informations - qu\'aux membres du Consortium. Nous disons : publiez le code source et tous les documents, sinon nous ne croirons rien de rien. Et pas seulement une quelconque implémentation de référence client, non : la spécification complète et le code-serveur en entier. Full docs or shut the fuck up !

Critique 1 : détails techniques.

Les détails suivants proviennent des rares informations du site internet du PEPP-PT et des nouvelles de netzpolitik.org

Les applications attribuent à chaque appareil un numéro d’identification (ID) momentanément valable, authentifié et généré au hasard. L’ID, temporaire et créé au hasard fonctionne comme un pseudonyme, lequel est censé protéger l’identité de manière fiable. Il est modifié à intervalles régulières (il est question de 30 minutes) et ne doit pas pouvoir être mis en relation avec le téléphone. Par la suite, personne n’est censé pouvoir a posteriori retrouver quelle personne se cachait derrière un tel pseudonyme. Chaque téléphone PEPP-PT (on entend par là un smartphone sur lequel l’application a été installée) envoie sur une courte distance, via la technique de réseau Bluetooth (baisse énergie : ang. BLE, Bluetooth-Low-Energy) son ID actuel, scanne en même temps son environnement et recense quels autres smartphones dotés du logiciel PEPP-PT-Software se trouvent à sa portée. Lorsque deux appareils se rapprochent, l’application enregistre l’ID temporaire de l’autre smartphone. Le rapprochement de téléphones d’autres utilisateurs de PEPP-PT est constatée par la mesure des signaux de réseaux (Bluetooth etc). Les données se maintiennent, au début, cryptées sur le smartphone, personne ne peut y avoir accès, soi-disant. En raison du peu d’information donné, la manière dont ce cryptage serait concrètement appliqué est encore incertaine. Chaque rapprochement n’est pas enregistré. C’est seulement lorsque le téléphone PEPP-PT A se trouve près du téléphone PEPP-PT B pour une durée « épidémiologiquement » suffisante (il est question de 15 minutes à 1,5m de distance), qu’alors l’identité temporaire du téléphone B est enregistrée dans l’historique de proximité (Proximity-Historie [sic]), crypté et sauvegardé localement sur le téléphone de A (et inversement).

La question suivante reste ouverte : est-ce que le choix de 15 minutes est une durée pertinente, puisque tousser sur quelqu’un dans le bus ou dans une boutique ne dure que quelques secondes, et un échange rapide une à deux minutes. Cela suffit pour une contamination. Ce qui est concrètement enregistré reste également incertain. Selon le site internet du PEPP-PT, aucune géolocalisation, aucune information personnelle, aucune identification individuelle d’appareil tel le numéro IMEI du smartphone ou autres données qui permettraient une identification de l’utilisateur ne seraient enregistrées. Il est encore prétendu que l’historique de proximité pseudonymisé ne peut être vu par personne, pas même par l’utilisateur du téléphone A. Les éléments plus anciens dans l’historique de proximité seront supprimés quand ils seront devenus inutiles d’un point de vue épidémiologique. “Nous mesurons seulement combien de temps et à quelle proximité deux personnes se sont rencontrées” dit Thomas Wiegand, qui dirige le HHI. Où la rencontre a eu lieu, cela n’intéresserait pas le virus. “Ce sont les seules informations qui ont un intérêt épidémiologique”. Après 21 jours, les données seront automatiquement supprimées. Plutôt que sur le Tracking, le PEPP-PT mise sur le Tracing : ce ne sont pas les déplacements des personnes mais seulement leurs contacts qui sont censés pouvoir être retracés. Sur le smartphone se dresse une liste des ID avec horodatages (ang. time stamp) derrière lesquels des personnes se cachent, que l’on peut avoir contaminées soi-même, ou bien desquelles on pourrait avoir attrapé le virus. Pour réduire les fausses alertes, les chercheu.rs/ses ont fait des recherches sur tous les modèles de smartphone les plus répandus et ont mesuré la force du signal de la technique de réseau, puisqu’elle est parfois différente. Les soldat.es de la Bundeswehr ont aidé à calibrer la technique de sorte à ce qu’elle reconnaisse, par exemple, s’il y a une vitre ou bien d’autres obstacles qui empêchent une transmission du virus entre les deux personnes en contact. Une exactitude fiable de la prévision de si quelqu’un.e

se trouvait dans un rayon de 1,5 mètres ou non au moyen du Bluetooth est particulièrement douteuse. Utilisation de l'historique de proximité Dans le cas où un.e utilisateur.trice n'est pas testé.e, ou bien a un résultat négatif au test, alors l'historique de proximité reste crypté sur le téléphone de l'utilisateur.trice et ne peut être vu par personne ni transféré. Cependant, s'il est avéré que l'utilisateur.trice du téléphone A est SARS-CoV-2-positi.f/ve (donc, en règle générale, qu'iel est déjà malade du Covid-19), alors cette personne est censée transférer sa liste des ID enregistrées jusqu'à ce jour dans son historique de proximité sur un serveur central national. Cela n'est pas possible sans condition. Les médecins, laboratoires et services administratifs de la santé doivent confirmer l'alerte. Il y a donc nécessairement besoin d'un diagnostic positif. Alors les services administratifs de la santé se mettent en contact avec l'utilisateur/trice A et mettent un TAN [numéro d'identification, ndlt] à sa disposition, lequel assure que de potentiels malwares [virus informatiques, ndlt] ne peuvent pas induire de fausses informations d'infection dans le système PEPP-PT. La connexion est censée fonctionner de manière cryptée et secrète, de sorte à ce que l'identité de la personne malade puisse rester protégée. L'utilisateur.trice utilise ce TAN pour transmettre volontairement des informations sur le serveur du fournisseur de service national, par exemple, en Allemagne, à l'Institut Robert Koch, qui rend possible d'envoyer une notification aux applications PEPP-PT qui sont inscrites dans l'historique de proximité et donc potentiellement infectées. Il est dit encore que tout cela se passerait de façon volontaire. Le serveur central n'apprend avec quelles autres ID temporaires tel Smartphone a été en contact uniquement si l'utilisateur.trice l'accepte. La pression sociale est occultée. Que se passe-t-il avec les données sur le serveur ? Le consortium écrit que, puisque l'historique de proximité contient des identificateurs sous forme de pseudonymes, le serveur ne serait pas en mesure de savoir, à partir de ces ID, quelles personnes se cachent derrière; cependant, il peut prévenir toutes les personnes concernées via l'application et les enjoindre à se faire tester. Cette notification peut alors être envoyée sans considération de qui est la personne utilisant le smartphone. En effet, pour afficher un message sur un smartphone, aucune donnée personnelle n'est nécessaire. En fait, ce qu'on appelle un Push-Token suffit, c'est-à-dire un identifiant unique d'appareil d'application, pour envoyer un message Push sur l'appareil via les Push-Notification-Gateways d'Apple ou de Google. Ce Push-Token est généré lors de l'installation de l'application sur le portable. En même temps, l'application stocke le Push-Token ainsi que les ID temporaires qu'elle émet au fil du temps sur un serveur central. De cette manière, on peut s'adresser directement aux seuls smartphones au moyen des ID temporaires et des Push-Token sans que l'identité des personnes qui portent ces smartphones sur elleux ne soit reconnaissable. Pour cela, il est cependant nécessaire que, pour chaque compte-usager, le Push-Token ainsi que toutes les ID temporaires qui ont été générées, y compris les horodatages du moment où ils l'ont été, soient stockés sur le serveur. On nous demande de faire confiance au fait que le serveur supprime après 21 jours les données non pertinentes d'un point de vue épidémiologique – et ne continue pas à les stocker pour les besoins des Big-Data. Dès le moment où l'on pourrait associer le Push-Token aux données du fournisseur d'accès (identification individuelle du Push-Token avec l'ID de l'appareil, l'IMEI ou le numéro de téléphone), alors une identification individuelle serait aisée.

Critique 2 : Anonymement aussi, on entraîne l'IA.

L'application PEPP-PT n'est pas censée avoir accès aux données personnelles des individus. Cependant le danger ne réside pas seulement dans la reconnaissance digitale des particuliers, mais aussi dans le fait que le stockage de données qui apparaît alors rend possible des méthodes algorithmiques de gestion de la population. Les masses de données pseudonymisées servent à l'entraînement de l'intelligence artificielle (IA), par exemple dans le contexte des analyses prédictives. Dès le moment où des données de comportement sont produites à assez grande échelle et sont collectée (même anonymement), alors les modèles de prédiction qui sont ainsi entraînés sont en mesure de catégoriser toute la population en groupes de risques et de la gérer par algorithmes. Les algorithmes basés sur les données peuvent alors catégoriser la société en classes sociales invisibles, par exemple en fonction de qui, en raison de son modèle de déplacements, représenterait soi-disant un risque sécuritaire ou sanitaire particulier, parce que son profil de déplacements révèlerait que quelqu'un.e aurait propagé le virus dans des proportions hors-norme, ou encore qui mérite un accès prioritaire aux ressources médicales telles l\'accès aux machines respiratoires. Les méthodes algorithmiques de scoring [accorder des points par rapport à un comportement spécifique, ndlt] et de décision sont basées sur la comparaison anonyme des données de beaucoup d'autres individus. De là, on peut, par la mise à disposition de ses propres données (bien qu'anonymisées ou pseudonymisées), potentiellement nuire à d'autres individus ou groupes et, réciproquement, être potentiellement soi-même touché.e par la mise à disposition des données d'autres personnes. Ce danger est occulté dans les débats raccourcis autour de l'application PEPP-PT et aussi, déjà, dans la mise à disposition de données de Telecom anonymisées ou de données de géolocalisation Google anonymisées. Ce même danger n'est pas non plus l'objet d'efforts efficaces en matière de droit et de protection des données. Ainsi, la DSGVO [Datenschutzgrundverordnung, la loi sur la protection des données, ndlt] ne protège pas de l'utilisation de données anonymisées pour des prises de décisions algorithmiques prédictives, ni des classifications de risque (scoring), ni

des inégalités de traitement des individus ou des groupes sur la base de leur comportement. Dans ce sens, chaque personne qui utiliserait l'application PEPP-PT participerait à une telle inégalité de traitement.

> *C'est là que nous dépassons la différenciation entre données anonymes et données personnelles : parce qu'elle n'est pas pertinente !*

Critique 3 : le "volontariat".

> *"Pour votre propre sécurité et pour la sécurité de nos collaborateurs/trices, nous ne pouvons transporter et servir que des personnes dont la non-contamination a été prouvée. Merci de votre compréhension."*

Telle pourrait être l\'annonce de la Deutsche Bahn [SNCF allemande, ndlt], sur tous ses automates et ses guichets, si elle proposait un service restreint "jusqu'à la fin de la crise du Corona" aux voyageu.rs/ses ayant une application PEPP-PT modifiée. L'application PEPP-PT 2.0 pourrait en plus (là encore, de manière absolument volontaire et seulement avec l'accord de l'utilisateur/trice) "sur demande" signaler tous les événements de contact directement sur le serveur – avec une sorte de Free-TAN. Il n'y aurait toujours aucune donnée personnelle, donc aucune géolocalisation enregistrée. Ce serait seulement lorsque le traitement des données en temps réel de tous les événements de contact des derniers 14 jours ne montrerait aucun lien avec une personne contaminée ni avec une personne qui aurait auparavant eu un contact avec une personne infectée, qu'un QR code sur le e-billet de train s'allumerait en vert, donc "probablement non contaminé". Cela signifie : feu vert, soit lors des contrôles des tickets soit lors de l'entrée même en gare [comme c'est déjà le cas à Wuhan, source : article de Libé "A Wuhan, la liberté toujours supendue à un QR Code", ndlt].

Les centres commerciaux, salles de concerts, stades, … pourraient sur le même principe limiter l'entrée ou le paiement en caisse à la condition de montrer un smartphone avec un statut d'application PEPP-PT "vert". Ce serait une limitation massive de la liberté de mouvement – qui veut être "libre" doit se soumettre à l'application (et à l'infrastructure du serveur qui la sous-tend). On peut comparer cela à un bracelet électronique : les personnes en liberté conditionnelle doivent le porter, ou alors retourner en détention.

L'application "volontaire" PEPP-PT devient en cela un outil de différenciation pour la participation individuelle sociale. Qui voudrait voyager en train aurait alors besoin de l'application PEPP-PT 2.0. L'Etat n'"ordonne" pas l'utilisation de cette application PEPP-PT élargie, il la rend seulement disponible. Les acteurs économiques – dans notre exemple, la Deutsche Bahn – ne proposeraient alors leurs services qu'à celleux qui auraient donné leur accord à cette variante prolongée de l'application PEPP-PT. Le gouvernement et les prestataires de services agiraient alors en cela tout-à-fait dans le sens de la priorisation de la responsabilité pour le bien commun. Qui voudrait s'en plaindre … ? C'est sur cette forme de "volontariat" que se basent actuellement les modèles éprouvés de scoring social en Chine. Qui ne participe pas, ou bien qui ne remplit pas les caractéristiques nécessaires (en ce qui concerne l'application en question, de ne pas être contaminé.e) peut, sans la moindre interdiction (administrative), être "volontairement" exclu.e de la vie publique : l'application PEPP-PT en tant qu'exercice des mécanismes d'inclusion/exclusion individuelle du futur système social à points, en Allemagne aussi. Un dernier aspect est que les données, dont il est promis qu'elles seront traitées de façon confidentielle, peuvent encore et toujours être utilisées pour des poursuites judiciaires et le débat à ce sujet n'arrêtera que lorsque l'accès à ces données sera autorisé. Là où il y a du grain, les poulets rappliquent. Des exemples (comme la reconnaissance des plaques d'immatriculation par les péages électroniques [utilisés entretemps en Allemagne et ailleurs dans le cadre de poursuites judiciaires, ndlt]), il y en a beaucoup. A cela s'ajoute le refus des services administratifs de supprimer les données qu'ils ont déjà collectées. Actuellement, les personnes doivent activement autoriser l\'accès aux données de leur historique de proximité. Mais avec une mise à jour du logiciel, on y remédie facilement, pour faire en sorte que tous les contacts soient téléchargés constamment. Se constitue ainsi d'un coup une énorme botte de foin, qui est utilisable pour les besoins des Big-Data. Si toutes les ID des contacts peuvent être analysées (donc plus seulement à condition qu'une personne soit contaminée), alors le serveur peut aussi construire des Traces et mettre en place des liaisons sur qui rencontre qui et à quel rythme. En collaboration avec les fournisseurs de télécommunication pour la résolution des adresses IP, les autorités judiciaires pourraient alors trouver qui se trouve derrière quelle ID.

capulcu, 5 avril 2020
traduit le 12 avril 2020
capulcu.blackblogs.org