Suivi numérique des contacts aux Etats-Unis : une multitude de dispositifs expérimentaux qui s'organisent pour converger

Le déconfinement de certains Etats amorcé en mai reposait sur une stratégie (dépister, tester, isoler) dont la mise en oeuvre était déléguée aux Etats. Le suivi des contacts est un élément clé de la stratégie de réouverture : il permet de retracer l'évolution de l'épidémie mais aussi de contribuer à limiter sa propagation dans un contexte où les porteurs asymptomatiques semblent être des vecteurs importants et où le nombre de tests disponibles est limité. La mise en œuvre d'un tel suivi repose avant tout sur des ressources humaines massives, mais le CDC recommandait officiellement l'utilisation, en complément, d'outils digitaux pour le réaliser et fournissait quelques consignes minimalistes[1].

Les outils numériques peuvent permettre d'améliorer le processus sans tout résoudre.

Ainsi les outils numériques pourraient faciliter le suivi mais, aux Etats-Unis comme en Europe, leur implémentation doit reposer sur le consentement des utilisateurs et donc leur inspirer un haut degré de confiance, d'autant plus qu'ils protègent peu leur utilisateur mais servent surtout la collectivité.

Trois niveaux techniques sont imbriqués : le type d'information collectée par les smartphones, le protocole d'échange des données et l'autorité de référence.

Niveau 1 : Information collectée par les

smartphones

Bien que certaines applications collectent la localisation de l'utilisateur à l'aide du GPS intégré à son smartphone et permettent ainsi de reconstituer ses déplacements, les solutions qui s'imposent de plus en plus se concentrent sur la collecte des « contacts », le plus souvent en exploitant un usage détourné de la fonction Bluetooth qui permet de déterminer la proximité relative entre deux utilisateurs, indépendamment de leur emplacement "absolu".

Cette approche soulève de nombreuses difficultés techniques (non encore optimalement résolues) qui peuvent compromettre l'efficacité du dispositif ainsi que des failles cyber (de faible portée) : l'évaluation de la distance et de la durée du contact à partir de la force des signaux, l'accès au Bluetooth pendant l'usage d'autres applications (notamment sous iOS), la surconsommation d'énergie, la compatibilité entre des appareils munis d'applis différentes (interopérabilité) et la restriction des données échangées par ce canal au strict nécessaire.

D'autres technologies pourraient être utilisées. Par exemple, la startup *Novid*, issue de Carnegie Mellon University, propose une alternative originale qui utilise en complément les ultrasons pour identifier les contacts[2].

Niveau 2 – Gestion des données

Une question essentielle, sur laquelle ont achoppé certains pays (FR et UK), est la question du stockage centralisé ou décentralisé des données. Une gestion centralisée (promue par la France), apporterait une souveraineté sur les données, ainsi qu'une possibilité d'exploiter les données à des fins épidémiologiques et un suivi plus rapproché avec les équipes de suivi de contacts manuel. Les données de contacts collectées par les applications basées sur l'utilisation du Bluetooth sont peu sensibles en elles-mêmes, mais, regroupées et couplées aux informations d'infection, elles pourraient permettre, si elles sont centralisées, d'identifier les personnes infectées par recoupements. Pour limiter ce risque, certains protocoles (on parle un peu abusivement de gestion décentralisée) proposent que ces données de contacts ne soient échangées qu'entre les smartphones. Dans ce cas, seules les informations sur les individus infectés passent par l'autorité centrale qui les valide et les

redistribue à tous.

Niveau 3 – Autorité pilotant le dispositif.

Elle est nécessaire, a minima pour valider les tests d'individus infectés et qui sont de ce fait reconnus comme potentiellement contagieux par l'application. Cela permet en outre d'éviter que des individus malveillants ne provoquent un grand nombre de faux positifs en se déclarant infectés. En tout état de cause ce niveau détermine les limites géographiques : c'est l'une des raisons pour lesquelles les applications sont développées au niveau national en Europe et au niveau fédéré, voire des comtés, aux États-Unis.

L'enjeu d'adoption par le public a fortement contraint les choix techniques.

Un débat très animé a commencé aux Etats-Unis, dès le mois de février dans les cercles spécialisés, sur l'opportunité du déploiement des applications de suivi numérique et leurs modalités. Le principe d'une utilisation sur la base du volontariat s'est imposé immédiatement. Dans ce contexte, il est peu vraisemblable d'atteindre un taux d'adoption permettant d'espérer éradiquer complètement l'épidémie : l'étude[3] estime qu'il faudrait détecter un tiers des contacts à risque et que pour cela il faudrait qu'au moins 60% de la population soit équipée. Dès lors, le message véhiculé par les promoteurs du suivi numérique est qu'un usage même partiel peut contribuer au ralentissement mais que le taux d'adoption reste un enjeu crucial pour son efficacité.

Il faut donc convaincre les utilisateurs potentiels, ce qui oblige à prendre en compte leurs attentes pour définir les spécifications techniques des applications. Dans cette optique, les universitaires ont recensé les enjeux et ont proposé des protocoles permettant d'y répondre. Une étude[4] publiée le 30 avril dernier, réalisée par Elissa M. Redmiles, chercheuse à l'Université du Maryland et chez Microsoft, recense les différents compromis entre choix techniques et inquiétudes des utilisateurs : collecte des données, qualité des données, cryptage des données d'identification, perte de

confidentialité, coût, organismes impliqués, bénéfices attendus, transparence.

La voix des associations de défense des libertés s'est imposée dans le débat public

Les organisations de défense des libertés et de la confidentialité des données ont publié une liste d'exigences que doit satisfaire toute application de suivi numérique (voir par exemple celles formulées par l'*American Civil Liberties Union* (ACLU)[5]) qui sont sur le fond assez similaires aux avis énoncés dans la délibération de la CNIL quand elle a été saisie par le secrétaire d'Etat au numérique concernant "StopCovid": l'installation doit être faite sur la base du volontariat, l'utilisation des données doit être limitée dans le temps et doit préserver la confidentialité des utilisateurs, etc. Certains des promoteurs de ces idées ont eux-mêmes contribué à l'élaboration de protocoles (par exemple John Callas de l'ACLU est l'un des rédacteurs du protocole proposé par le MIT, voir *infra*). Mais finalement, la plupart des développeurs d'applications de suivi de contacts se sont appropriés ces exigences et les ont mises en oeuvre, de même qu'Apple et Google par la suite. Elles sont ainsi devenues un cadre de référence aux Etats-Unis, intégrant en particulier, la réticence à centraliser les informations, y compris de contact, qui est apparue très tôt dans le débat.

La promotion de l'idée auprès du grand public : les réactions de la population sont mitigées.

Plusieurs études[6][7] réalisées en avril tirent un bilan cohérent des réactions du public : parmi les 80% des américains disposant d'un smartphone, seule une moitié serait disposée à s'équiper d'une application de suivi. Le taux d'adoption serait très corrélé à la peur inspirée par la maladie (parmi ceux qu'elle n'inquiète pas particulièrement, seuls 35% seraient prêts à utiliser une appli, alors qu'il s'agit probablement des personnes les plus à risque car moins précautionneuses), et est aussi corrélé à la couleur politique (seuls 38% des républicains l'utiliseraient, contre 61% des démocrates). Ces études montrent également qu'une majorité des américains fait peu confiance aux grandes plateformes numériques telles qu'Apple ou Google (43%

d'opinions favorables) et peu confiance aux compagnies d'assurance (47%). Au contraire, les universités et agences de santé publique ont la confiance de respectivement 56% et 57% des américains sondés. Enfin, un autre sondage réalisé par la Kaiser Family Foundation[8] souligne l'importance de la confiance pour le déploiement de ces applications de traçage en notant que seulement 31% des sondés seraient prêts à télécharger une application si elle était gérée par une plateforme numérique contre plus de 60% si elle l'était par les départements de santé (local, Etat ou fédéral) ou le CDC.

Un projet de loi pour protéger les données des usagers

Un groupe de sénateurs républicains mené par Roger Wicker (Président de la Commission du Commerce) a annoncé le 30 avril qu'ils allaient proposer un projet de loi[9] visant à protéger les données des utilisateurs d'applications d'aide au suivi des contacts. Ils souhaitent notamment « rendre les entreprises responsables vis-à-vis des utilisateurs si elles utilisent leur données ». Ce type de réglementation contraignante n'est pas la norme aux Etats-Unis et montre qu'en cette situation exceptionnelle, une attention particulière est portée au suivi numérique des données au niveau fédéral ; cette loi vise manifestement à rassurer le grand public et à encourager à adopter des outils de suivi numérique lors de la phase de déconfinement.

Les sénateurs démocrates ont proposé de leur côté un projet ayant les mêmes objectifs mais se voulant plus strict dans le contrôle imposé. Il semble que les deux partis aient réussi à s'entendre début juin.

Les principaux acteurs s'adaptent à un paysage qui se précise petit à petit.

En l'absence d'un pilotage fédéral volontariste, la recherche d'un compromis entre efficacité et respect des libertés s'effectue aux Etats-Unis avec un temps de retard sur l'Europe : les Etats tranchent en fonction de leur sensibilité et des partenaires

locaux (universitaires, startup ou autres développeurs) avec lesquels ils peuvent implémenter des solutions. Cette situation conduit au développement d'un patchwork de dispositifs expérimentaux sur tout le territoire américain mais qui commence à se structurer.

Convergence vers un type de solution modulaire.

Ainsi, dans le Dakota du Nord, l'application de traçage *Care19* utilisant la géolocalisation est disponible au téléchargement sur les plateformes d'Apple et Google depuis le début du mois de mai. Dans l'Utah, le gouverneur Gary Herbert a annoncé dès le 22 avril la sortie d'une application (*Healthy Together*) en version test. A l'inverse, l'Etat d'Indiana a explicitement décidé de ne pas promouvoir d'application digitale et organise le suivi de contacts de façon exclusivement manuelle.

Mais sous la pression des associations, des universitaires et du public, le cahier des charges attendu pour les applications de suivi numériques s'est clarifié : celles-ci doivent être installées sur la base du volontariat et de l'anonymat, sans partage de localisation, bénéficier d'un haut niveau de confidentialité, et prévenir toute possibilité de fuite de données. Cela tend à promouvoir les technologies basées sur le Bluetooth, ainsi qu'une gestion décentralisée des données qui doivent rester autant que possible sur les smartphones des utilisateurs.

La séparation des niveaux (information collectées / protocole d'échange des données / autorité compétente) produit une modularité qui permet en principe le développement de multiples applications entre lesquelles, au delà de l'enjeu d'une adoption suffisante pour atteindre une certaine efficacité, on doit assurer une « inter-opérabilité » : d'une part les appareils en « contact » mais munis d'applications distinctes doivent pouvoir s'identifier (niveau 1) et d'autre part les protocoles de dialogue (niveau 2) entre les smartphones et avec les autorités locales (niveau 3) doivent être compatibles. Cela ne semble pas poser de difficultés techniques insurmontables et une convergence des multiples projets en cours aux Etats-Unis a l'air envisageable.

Les porteurs des projets les plus aboutis ont fait évoluer leurs propositions dans la même direction

De nombreuses initiatives se sont développées aux Etats-Unis pour mettre au point des applications de suivi (voir document en annexe pour une liste détaillée). Ce poste est entré en contact avec 3 pôles particulièrement structurés qui se sont formés autour de projets indépendants (au MIT, à Stanford et à l'Université de Washington), qui proposent chacun une interface distincte mais sont en contact étroit et qui ont finalement des spécifications techniques relativement proches. Une liste plus exhaustive des initiatives identifiées en mai est présentée en Annexe.

Private Automated Contact Tracing (PACT)[10]

Le MIT a été précurseur sur le sujet : le chercheur Ramesh Raskar a développé la technologie *SafePaths*[11] qui se basait initialement sur le GPS et le Bluetooth de manière sécurisée. Avec l'apparition des exigences citées précédemment, cette technologie a été retravaillée pour devenir *Private Automatic Contact Tracing* qui n'utilise plus le GPS. Le projet maintenant piloté par Ronald L. Rivest et Danny Weitzner implique notamment Carnegie Mellon University et Brown University. Ce standard technique a été conçu, comme nous l'a expliqué Danny Weitzner, avec la préoccupation de préserver la vie privée grâce à l'utilisation de techniques de cryptographie et de faciliter l'interopérabilité avec d'autres systèmes. Il est en principe Apple/Google-compatible mais prévoyait initialement la possibilité de remonter des informations détaillées à l'autorité centrale avec le consentement de l'utilisateur.

COVID-WATCH[12] & TCN-Coalition[13].

Ce projet s'est développé autour de Tina White (chercheuse IA de l'Université Stanford). Il implique maintenant des partenaires de l'Université de Waterloo au Canada. Il se structure autour d'une association (*non-profit*) et se place ouvertement dans une perspective internationale en rejoignant le groupement « TCN-Coalition ». Comme nous l'a fait remarquer Mme White, les principes retenus sont extrêmement proches, notamment en termes de confidentialité de ceux que sont en train d'imposer Google et Apple (l'équipe avait travaillé aussi sur le GPS mais a choisi de

le mettre de côté assez tôt pour se concentrer sur la collecte des contacts Bluetooth). L'équipe est aussi en contact avec les chercheurs du MIT. L'application a été mise en test sur le campus de l'Université d'Arizona à la fin du mois de mai..

West Coast PACT[14]

En parallèle s'est développé à l'Université de Washington en lien avec Microsoft le *Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing* (West-Coast PACT, pour distinguer du PACT du MIT). Ce protocole, développé indépendamment et directement en vue d'un usage Bluetooth, est très similaire aux deux précédents. Shyam Gollakota, Professeur associé à UW et l'un des leader du projet insiste sur la complémentarité entre les outils numériques et le travail effectué par les équipes de traceurs. Leur application *CovidSafe* est disponible sous Android depuis la mi-avril et sous iOS depuis la mi-mai.

Les trois projets sont finalement très proches en termes de philosophie, et aussi semble-t-il sur de nombreux détails techniques. Ils se rapprochent également du protocole DP-3T européen. Leurs auteurs semblent appeler de leurs voeux une véritable convergence des standards, ce qui pourrait faciliter aussi une interopérabilité transfrontalière.

Parmi les autres initiatives identifiées dans l'Annexe, mentionnons l'application *Coalition* développée par la startup *Nodle.io* installée à San Francisco ; celle-ci avait déjà mis son expertise du Bluetooth au service du développement d'une autre application. *Coalition,* qui est basée sur un protocole développé pendant le confinement (*whisper tracing*), est disponible sous android et sous iOS. Son responsable, Micha Benoliel, un francophone qui a interagi avec INRIA (il participe au consortium autour de l'application française), estime pour sa part qu'il est possible d'utiliser suffisamment le Bluetooth sans se soumettre au cadre imposé par Apple (voir *infra*) ; il précise que le contact direct des développeurs avec Apple n'est pas facile à cause de la culture du secret entretenue par l'entreprise.

L'entente Apple + Google impose ses conditions

Si Apple et Google se sont entendus fin mars pour proposer une boîte à outils permettant d'assurer l'interopérabilité d'applications développées sous leurs deux

systèmes d'exploitation, ils ne développent pas eux-mêmes d'application de suivi.

C'est dans ce contexte qu'ils ont lancé le 29 avril les versions beta de leurs outils pour permettre aux développeurs d'applications d'adapter leurs logiciels. Les discussions qui ont suivi leurs annonces les ont amenés à modifier quelques unes des spécifications permettant par exemple de partager la durée et la « force » du signal Bluetooth et autorisant à mémoriser la date des contacts ; ils ont aussi amélioré le protocole de sécurité produisant les codes aléatoires associés à l'enregistrement des données utilisateurs Bluetooth, répondant ainsi à des critiques émises sur la proposition initiale.

Concrètement, l'usage de leur solution permet notamment d'accéder beaucoup plus facilement aux possibilités offertes par Bluetooth (notamment sous iOS) et de mieux synchroniser la communication au niveau 1. Mais la facilité offerte est conditionnée par l'adoption d'un protocole cryptographique décentralisé (niveau 2), interdisant la communication des informations de contact (même sous forme cryptée) à l'autorité pilote. Les raisons qui poussent Apple à imposer ce choix ne sont pas explicites : il semble s'agir d'une question d'image : le peu de crédit dont disposent les grands groupes américains de type GAFA quant à l'usage qu'ils font (ou laissent faire) des données de leurs utilisateurs les amènent à surjouer la protection ; cela mène à une situation paradoxale où ils apparaissent plus exigeants que les Européens sur ce plan…

Mais la plupart des interlocuteurs contactés estiment que la contrainte imposée par Apple et Google ne leur pose pas de problèmes ; par exemple Tina White estime que ces contraintes correspondent à celles que l'équipe de Covid-Watch s'étaient déjà imposées initialement. D'autres interlocuteurs sont plus pragmatiques et estiment que la visibilité du consortium Apple+Google sera un facteur d'adoption plus que de rejet par le grand public. Ainsi, la contrainte apportée par cet accord qui suit les tendances issues des débats du monde universitaire, semble jouer au final un rôle unificateur.

Conclusion

Le débat sur les applications de suivi des contacts pour accompagner le déconfinement a pris très tôt de l'ampleur en Europe alors qu'il est longtemps resté restreint aux cercles spécialisés aux Etats-Unis. Il a cependant fini par devenir un sujet bien suivi par la presse américaine.

L'annonce de l'alliance inédite entre Apple et Google visant à favoriser l'interopérabilité d'applications développées sous leurs deux systèmes d'exploitation a eu pour effet de faire converger les différentes initiatives issues du monde universitaire ou d'entreprises du numérique.

Pourtant, le positionnement qu'on pourrait qualifier de "privacy-washing" de ces deux géants crée une situation paradoxale : ils se présentent comme plus protecteurs encore que les promoteurs, en Europe, de la RGPD ! Cela s'explique probablement par leur volonté de redorer une image largement ternie sur ces aspects auprès de la population américaine.

Pour autant, l'efficacité de ces outils demeure aujourd'hui incertaine et leur impact n'apparaîtra que sur la durée. Si leur efficacité est encore incertaine, la plupart de nos interlocuteurs ont estimé que le travail effectué à l'occasion de la crise trouvera de toutes façons des applications à moyen terme. Tous ont rappelé que ces applications de suivi numérique des contacts ne sont qu'un outil dans une panoplie qui pourrait s'étoffer selon la tournure prise par l'épidémie.

Annexe : applications de suivi identifiées en mai 2020

Rédacteurs : Jean-Baptiste BORDES (SST San Francisco), Xavier BRESSAUD et Kevin KOK HEANG (SST Washington)

Notes :

1 https://www.cdc.gov/coronavirus/2019-ncov/php/open-america/contact-tracing.html

2 https://www.novid.org/#howitworks

3 https://science.sciencemag.org/content/368/6491/eabb6936

4 https://arxiv.org/pdf/2004.13219.pdf

5 https://www.aclu.org/sites/default/files/field_document/aclu_white_paper_-_contact_tracing_principles.pdf

6 https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/

7 https://www.washingtonpost.com/context/washington-post-university-of-maryland-national-poll-april-21-26-2020/

8 https://www.kff.org/global-health-policy/issue-brief/kff-health-tracking-poll-late-april-2020/

9 https://www.commerce.senate.gov/2020/4/wicker-thune-moran-blackburn-announce-plans-to-introduce-data-privacy-bill

10 https://pact.mit.edu/

11 https://www.media.mit.edu/projects/safepaths/overview/

12 https://www.covid-watch.org

13 https://www.tcn-coalition.org/

14 https://arxiv.org/pdf/2004.03544.pdf