Sur Le site de la Quadrature du net il y a deux articles à lire absolument si l'on veut fourbir ses arguments contre le projet, pour l'instant abandonné, de surveillance numérique de la population en période de dé confinement. Des arguments qui ne dénoncent pas seulement une dérive malheureuse vers la surveillance généralisée et attentatoire aux libertés individuelles, mais encore un mensonge politique et une arnaque technologique de plus.
Voici deux extraits éloquents des articles dont je vous invite à poursuivre la lecture ici et là.

La CNIL s'arrête à mi-chemin contre StopCovid

L'application StopCovid ne fera finalement pas l'objet d'un vote à l'Assemblée nationale, le gouvernement se refusant à tout risque de vote contraire à sa volonté. Pourtant, les prises de position s'accumulent contre elle et son avenir semble chaque jour plus incertain.

Hier, la CNIL a rendu son avis à son sujet. Contrairement au Conseil national du numérique (CNNum) qui s'est prononcé vendredi en faveur de l'application, la CNIL n'a pas entièrement fui le débat : elle exige que le gouvernement démontre l'utilité concrète de StopCovid, ce qu'aucune étude ou analyse ne soutient actuellement. Hélas, alors que la CNIL aurait dû s'arrêter à ce simple constat pour demander l'arrêt de ce dangereux et inutile projet, elle s'est égarée dans le faux-débat tendu par le gouvernement : rechercher des « garanties », forcément illusoires, pour encadrer l'application.
Une nécessité non démontrée

L'idée au cœur du droit des libertés fondamentales est que, par principe, il est interdit de limiter nos libertés. Elles ne peuvent l'être que par exception, et uniquement en démontrant qu'une telle limitation est utile à un intérêt supérieur, telle que la santé publique dans notre cas. Hier, la CNIL a rappelé ce principe cardinal, qu'elle applique naturellement de longue date. Par exemple, dans son avis sur les portiques de reconnaissance faciale dans des lycées de la région Sud, elle avait bien rappelé qu'il revenait au responsable de traitement de données« d'évaluer la nécessité et la proportionnalité du traitement envisagé ». Un tel raisonnement l'avait conduit à considérer que le projet de reconnaissance faciale était contraire au RGPD, car la région n'avait pas démontré cette nécessité.

Il ne fait pas de doute que StopCovid est une mesure limitant les libertés fondamentales, ce que la CNIL reconnaît facilement : risques d'attaques malveillantes, de discriminations, d'accoutumance à la surveillance constante, de dévoiement par le gouvernement. La CNIL exige donc que les prétendus bienfaits sanitaires de l'application soient démontrés avant que celle-ci ne soit déployée, ce qui fait jusqu'ici défaut. La rigueur du raisonnement de la CNIL tranche nettement avec l'avis du CNNum, qui conclut en faveur de StopCovid hors de toute méthode d'analyse sérieuse.

Toutefois, il faut regretter que la CNIL se soit arrêtée là, sans conclure et répondre elle-même à la question qu'elle a si justement posée. Si aucun élément factuel ne prouve l'efficacité d'une technique qu'elle reconnaît pourtant comme attentatoire aux libertés fondamentales, la mission de la CNIL est de déclarer celle-ci illégale. Déclarer illégaux des traitements de données injustifiés est une des missions centrales qui justifient l'existence de la CNIL.

Mais, refusant de tenir son rôle, la CNIL s'est ensuite perdue dans le débat vain souhaité par le gouvernement : chercher à tâtons les garanties pouvant encadrer cette pratique. Pourtant, les conditions pour que StopCovid respecte nos libertés sont impossibles à remplir. L'essence même du « traçage de contact », automatique comme manuel, rend impossible l'anonymat, et le contexte de crise sanitaire rend irréaliste la garantie d'un consentement libre.
Un anonymat impossible

Cédric O affirme que les données traitées par StopCovid « seraient anonymes ». De même, Bruno Sportisse, directeur de l'INRIA chargé du protocole ROBERT sur lequel reposera l'application, affirme que celle-ci serait « totalement anonyme ».

En pratique, une application anonyme n'aurait aucun intérêt : l'application doit envoyer à des personnes ciblées des alertes du type « vous avez été au contact de personnes malades, mettez-vous en quarantaine ». Du moment que chaque alerte est envoyée à des personnes ciblées, le système n'est plus anonyme : trivialement, il suffit qu'un tiers (un patron, un conjoint, etc.) puisse consulter votre téléphone pour constater que vous avez reçu une alerte. Des chercheu·ses de l'INRIA ont produit une excellente liste de quinze scénarios de ce type, démontrant à quel point il était simple de lever ce prétendu « anonymat ».

Hélas, le CNNum s'enfonce dans le déni de réalité et continue de prétendre que « les utilisateurs de l'application ne peuvent pas se réidentifier entre eux ». Dans une étrange note de bas de page, l'avis du CNNum admet que cette affirmation est peut-être fausse puis renvoie vers les scénarios de l'INRIA. Voilà la triste posture du CNNum : mentir dans le corps du texte et s'excuser en pied de page, en petits caractères.

De son côté, heureusement, la CNIL est plus honnête et ne cache pas ces failles : les données traitées par StopCovid sont des pseudonymes ré-identifiables. Mais elle refuse d'en tirer la moindre conséquence effective. Après avoir exigé quelques mesures de sécurité nécessaires qui ne changeront pas le fond du problème, elle semble se bercer dans l'illusion que le droit serait une garantie suffisante pour empêcher que ce pseudonymat si fragile ne soit levé. Au final, sa seule « garantie » n'est rien d'autre que ce cher RGPD que la CNIL échoue à faire respecter depuis deux ans, quand elle ne s'y refuse pas carrément (lire notre article sur les cookies publicitaires).
(…)

Nos arguments pour rejeter StopCovid

Une efficacité hasardeuse, une utilisation trop faible

de premières approximations évaluent que plus de 60%1, voire plutôt 80% ou 100% de la population devrait utiliser l'application pour que celle-ci soit efficace, à condition encore qu'elle produise des données fiables ; seulement 77% de la population française a un smartphone et cette proportion baisse à 44% pour les personnes de plus de 70 ans, alors qu'elles sont parmi les plus vulnérables; beaucoup de personnes ne savent pas forcément activer le Bluetooth et certaines refusent de le maintenir activé en permanence pour des raisons pratiques (batterie) ou pour se protéger d'usages malveillants2 ; 16% de la population de Singapour a utilisé l'application équivalente – ce qui n'a pas empêché de devoir finalement recourir au confinement.

Résultats trop vagues

il faut redouter que la population n'ait pas accès à des tests de façon assez régulière pour se signaler de façon suffisamment fiable (et se reposer uniquement sur l'auto-diagnostic risquerait de faire exploser le nombre de faux-positifs) ; il ne semble n'y avoir aucun consensus quant à la durée et la distance de proximité justifiant d'alerter une personne entrée en « contact » avec une autre personne contaminée; à certains endroits très densément peuplés (certains quartiers, grandes surfaces, grandes entreprises) on assisterait à une explosion des faux positifs, ce qui rendrait l'application inutile ; le champ de détection du Bluetooth semble beaucoup trop varier d'un appareil à un autre et sa précision n'est pas forcément suffisante pour offrir des résultats fiables.
(…)