Démocratie numérique

Les leçons d'une crise sanitaire

Florimond Houssiau, **Mark Hunyadi**, **Steve Tumson**
Membres du collectif AlterNumeris
https://www.alternumeris.org/

Florimond Houssiau *est Ingénieur civil en mathématiques appliquées et doctorant dans le département Computational Privacy de l'Imperial College London.*

Mark Hunyadi *est professeur de philosophie morale et politique (UCLouvain), membre du centre de recherche en robotique médicale Louvain Bionics et auteur de plusieurs ouvrages sur la thématique du numérique.*

Steve Tumson *est Ingénieur civil spécialisé en robotique, consultant, conférencier et professeur.*

Résumé

La crise sanitaire causée par le Covid-19 a généré de nombreux tremblements dans différents pans de la société belge, ainsi qu'autour du globe. Dans le domaine des technologies, elle a fait couler de l'encre autour du recours aux outils numériques pour contrer l'expansion du virus. Ce dossier fait état des enjeux liés à l'usage de ces technologies dans l'actualité du débat belge. Il tire trois enseignements de cette crise qu'il envisage comme symptomatique des politiques actuelles du numérique : (1) **le temps du numérique ne peut pas être celui de l'urgence**, (2) **des principes fondamentaux** doivent encadrer la conception et l'utilisation des nouvelles technologies numériques et (3) **une interface solide entre technologie et société est indispensable**. De ces leçons apparait la nécessité de se doter des capacités institutionnelles permettant de poser les fondements d'une véritable démocratie du numérique.

I. Crise sanitaire et outils numériques De quoi parle-t-on?

Depuis mi-mars en Belgique, et plus tôt encore dans d'autres pays, l'épidémie causée par le Covid19 s'est installée, amenant avec elle des conséquences sans précédent sur nos vies personnelles, professionnelles, notre économie, et notre société dans l'ensemble. Nombre d'entre nous avons été soumis à des mesures de confinement qui auraient semblé inimaginables quelques mois auparavant, alors que le pays tout entier attendait que le nombre de cas de contamination diminue.

Au fil des semaines, le rôle des technologies numériques a émergé subitement dans la gestion de la crise en tant qu'instrument de mesure et de limitation de la propagation du virus. Il s'agit notamment de s'appuyer sur des systèmes qui identifient les personnes à tester suite à leur contact rapproché avec des personnes infectées, ou permettent aux personnes susceptibles d'être infectées de continuer à communiquer ou d'être suivies médicalement tout en étant isolées. Ces systèmes peuvent être numériques (via une application sur nos téléphones 'intelligents') ou manuels (via des centres d'appels), et une collecte massive de données est nécessaire pour les alimenter. Plus largement, au-delà de ce niveau individuel, il est attendu des données collectées par le recours à ces outils d'analyser les tendances et les évolutions de la pandémie à un niveau plus large.

PRINCIPAUX REPÈRES DE LA CONSTRUCTION DU CADRE DESTINÉ À BALISER LES DISPOSITIFS DE TRACING (AU 16/09/20)

⇒ **4 février 2020** : Premier cas de COVID-19 en Belgique

⇒ **10 mars** : Deux entrepreneurs en Big Data écrivent une carte blanche pour inciter le gouvernement à utiliser les données de la population recueillies par les opérateurs de télécommunication, pour le bien public[1].

⇒ **15 mars** : Le Ministère de la Santé et le Ministère en charge du numérique créent le groupe de travail "Data Against Corona", qui analysera ces données pour guider les phases de (dé)confinement de la population[2], ce qui sera fait pendant 2 mois[3].

⇒ **8 avril** : Le groupe de travail "Data Against Corona" se penche sur une application de traçage sur téléphones intelligents[4].

⇒ **22 avril** : Proposition de Résolution déposée pour encadrer le développement potentiel d'une application numérique de traçage sur téléphones intelligents.

⇒ **23 avril** : Le ministre fédéral De Backer annonce qu'une application de traçage n'est pas nécessaire, et renvoie la décision aux Régions qui devront chacune décider de leur stratégie[5].

⇒ **25 avril** : Lors de la conférence de presse officielle, le gouvernement fédéral annonce que le traçage se fera manuellement, via des centres d'appels[6].

⇒ **30 avril** : L'Autorité de Protection des Données (ADP) renvoie un avis négatif sur deux projets d'Arrêtés Royaux portant respectivement sur l'utilisation d'applications de traçage et sur la constitution d'une base de données afin de prévenir la propagation du coronavirus[7]. Personne n'avait connaissance de ces deux projets, même le Parlement semble surpris[8], d'autant plus que le dispositif de traçage numérique ne semblait plus d'actualité.

⇒ **04 mai** : Publication au moniteur belge de l'arrêté royal de pouvoirs spéciaux n° 18 portant sur la création d'une base de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19. Un nouvel arrêté royal n° 25 du 28 mai 2020 en prolongera les effets et le délai de conservation des données respectivement jusqu'au 30 juin et au 5 juillet.

⇒ **05 mai** : Entrée en vigueur de l'arrêté du Gouvernement wallon de pouvoirs spéciaux n° 35 organisant le tracing socio-sanitaire dans le cadre de la lutte contre l'épidémie COVID-19. Le texte vise à organiser la collecte des informations sur les personnes testées positives et celles avec qui elles ont été en contact.

⇒ **13-14 mai** : Deux propositions de loi sont déposées à la Chambre afin de lutter contre la propagation du COVID-19. Une portant sur la création d'une banque de données auprès

de Sciensano (pour le traçage manuel) et l'autre relative à l'utilisation d'applications numériques de traçage de contacts (pour le traçage numérique).

⇒ **26 mai** : La presse annonce qu'une application de traçage serait d'usage dès le mois de juillet, développée par un nouveau groupe de travail interfédéral[9], et ce, malgré l'activité très faible des centres d'appel de traçage manuel[10]. En parallèle de cela, le Conseil d'Etat publie un avis, dans lequel il mentionne, entre autres, que le traçage relevait tant des compétences du fédéral que des entités fédérées et recommande de passer par un accord de coopération.

⇒ **2 juin :** Publication au moniteur du décret flamand portant organisation de l'obligation de déclaration et du suivi des contacts dans le cadre du COVID-19. Le texte aménage la mise en place d'un centre de contact chargé de missions de traçage et d'accompagnement de personnes diagnostiquées du COVID-19 et des contacts à risques.

⇒ **18 juin** : Le gouvernement fédéral et les entités fédérées ont jeté les bases d'un accord de coopération réglant le traçage manuel et numérique[11].

⇒ **26 juin** : A défaut de pouvoir conclure et ratifier un accord de coopération avec tous les parlements avant la date du 30 juin, l'arrêté royal de pouvoirs spéciaux n°44 est publié au Moniteur belge afin d'éviter un vide juridique. Il prolonge jusqu'au 15 octobre la durée de validité de la banque de données utilisée dans le cadre du traçage et pose également les bases juridiques de l'utilisation d'une application numérique.

⇒ **juillet** : Un appel d'offre est lancé pour développer l'application numérique de traçage et ne reçoit que deux candidatures. La société bruxelloise DevSide est finalement sélectionnée[12]. Les choses se précisent et on connait le nom de l'application de traçage : Coronalert.

⇒ **5 août** : Comme l'impose le Règlement Général de Protection des Données (RGPD), une consultation publique est ouverte par le groupe de travail interfédéral en charge du développement de Coronalert. Elle se clôture le 31 août.

⇒ **10 septembre** : Le Groupe de Travail Interfédéral annonce que l'application sera disponible dans la semaine du 28 septembre, alors que le cadre légal est encore flou.

Durant toute cette période, l'Autorité de Protection des Données et le Conseil d'Etat ont parfaitement joué leur rôle en publiant une série d'avis portant sur les propositions de textes visant à encadrer les dispositifs de traçage[13]. Leurs travaux, parfois durs à l'égard des textes déposés, rappellent son importance dans le processus législatif pour œuvrer au respect des principes fondamentaux qui sous-tendent le recours à la collecte de données en général et l'utilisation de l'instrument numérique en particulier. Si cet épisode démontre l'enchevêtrement complexe des différents niveaux de pouvoir pour traiter de la matière dont question, on

retiendra surtout les hésitations relatives à la mise en place d'une application de traçage numérique. D'abord annoncée, puis remplacée par des centres de collecte, elle est finalement annoncée de nouveau à la fin du mois de mai et prévue pour fin septembre dans un cadre juridique encore flou.

Comment fonctionnent les applications de traçage ?

Les métadonnées téléphoniques contiennent de l'information sur notre position (imprécise) dans le temps. En clair, il s'agit d'informations récoltées par les opérateurs téléphoniques lorsqu'un utilisateur reçoit/envoie un SMS ou un appel. Typiquement, elles sont constituées du numéro des deux utilisateurs, l'heure, et l'endroit où se situe chacun d'eux. Ces données sont hautement identifiables : connaître quelques points (endroit + heure) est souvent suffisant pour identifier uniquement quelqu'un.

Ce sont des données très sensibles, car elles peuvent révéler beaucoup d'informations sur notre vie privée. On les utilise de façon agrégée pour essayer de mesurer les mouvements de population et évaluer l'efficacité des mesures de confinement. Par exemple, Google a publié des rapports agrégés mesurant la diminution de mobilité causée par les mesures gouvernementales à travers le monde, dans le but d'aider à la décision. Les opérateurs téléphoniques ont également accepté de partager leurs données agrégées anonymes avec l'État, avec (potentiellement) un plus grand niveau de détail. Cela permet par exemple de détecter quels lieux publics (rue commerçante, parc…) sont trop fréquentés et doivent être fermés.

Le traçage de proximité : quand une personne est diagnostiquée positive, toutes les personnes qu'elle a rencontrées (et potentiellement infectées) durant les deux dernières semaines sont averties et mises en quarantaine. Le traçage de proximité est une technique standard pour limiter la propagation, et a par exemple été employée dans la lutte contre Ebola. Dès lors que ce traçage est fait efficacement au moyen d'une application que beaucoup de gens installent, on peut rouvrir le pays sans risque de voir exploser le nombre d'infectés. Ce « traçage des contacts » peut s'effectuer soit par l'intervention directe de personnes habilitées (au travers d'un centre d'appel), soit en utilisant des applications numériques permettant notamment de détecter et de mémoriser automatiquement la proximité de deux smartphones que l'on suppose être portés par deux personnes, ou encore en combinant les deux approches.

II. Les enjeux et les axes de tension

L'introduction de ce type de système n'est pas sans créer des tensions au sein des sociétés, des frictions dont il nous appartient d'être attentif non seulement pour prévenir les éventuelles dérives liées à l'introduction des technologies numériques, mais également pour s'assurer de leur **appropriation citoyenne** et de leur véritable efficacité à long terme. L'analyse des débats récents fait émerger différents types d'enjeux et axes de tension.

1. Du point de vue de la protection de la vie privée

Le **Règlement Général de Protection des Données (RGPD)** empêche-t-il l'Europe de protéger ses citoyens en entravant l'emploi des données pour mesurer et contrôler l'impact du virus ? Non. Le RGPD permet une exception en cas de pandémie, sous la condition que l'utilisation des données soit faite « dans l'intérêt du public ». Il importe dès lors que cette notion puisse être suffisamment balisée pour pouvoir, dans les cas d'urgence tels que prévus par le RGPD, mettre à disposition des acteurs impliqués une définition claire et opérationnelle de ce qui est acceptable.;

Conformément à cette exigence, l'European Data Privacy Board (EDPB) a expliqué dans une publication qu'une telle **exception** n'est justifiée que si elle est « nécessaire, appropriée et proportionnée dans une société démocratique ». Par exemple, le partage des métadonnées téléphoniques avec l'État pour évaluer la mobilité des gens doit se faire de façon anonyme ou avec le consentement explicite de la population. En Belgique, l'Agence de Protection des Données (ADP) a récemment publié un rapport soulignant l'importance de démontrer la nécessité et la proportionnalité des applications de traçage.

2. Du point de vue technique

Un débat technique a lieu autour de comment concevoir une application de traçage: les solutions centralisées (à la Française), où une autorité centrale s'occupe de contacter les personnes, et les solutions décentralisées (telles que DP3T soutenues par Google et Apple), où chaque téléphone apprend au travers d'informations chiffrées si il a été en contact avec une personne infectée. Les deux comportent des risques et compromis différents, et le choix entre l'une et l'autre doit se faire de façon **transparente et démocratique**. Cela s'applique aussi au traçage manuel: quelles données jugeons-nous acceptables de partager avec des institutions et compagnies (sachant que bien souvent, elles ne sont pas anonymes).

A ce stade, personne ne sait réellement si une application de traçage est **efficace** pour endiguer l'épidémie. Selon une étude de l'université d'Oxford, une adoption de l'application par au moins 60% de la population permettrait d'éliminer la transmission du virus, sous hypothèses de tests nombreux et de quarantaine stricte. Les résultats de l'étude montrent que même une installation moins répandue de l'application permettrait d'endiguer la propagation du virus, mais ce n'est pas encore clair à quel point ces résultats s'appliquent à la réalité. De même, les **faux positifs et faux négatifs** peuvent avoir des conséquences graves. D'une part, l'application peut conférer un sens de confiance excessive, et des personnes infectées mais non détectées pourraient répandre plus facilement le virus. D'autre part, les personnes marquées comme potentiellement à risque risquent d'être obligées de restreindre leur mobilité et contacts sociaux sans réelle raison, ce qui peut représenter un coût réel.

Même si la collecte de données (par une application ou un centre d'appel) est bien conçue du point de vue de la protection de la vie privée, elle pose un problème important, celui de la **fuite des données**. Par le fait de hackers organisés ou en raison d'une erreur humaine, les données collectées par une application peuvent fuiter. L'expérience montre que ce risque n'est pas à négliger (pensons aux fuites de données massives de ce type d'application en Allemagne et au Qatar).

3. Du point de vue éthique

Le **consentement** des gens à l'emploi de leurs données personnelles est un enjeu important. Les applications de traçage de contact sont un bon exemple : l'installation d'une telle application doit être laissée à la volonté de tout un chacun. Le consentement à l'utilisation doit être garanti, contre toute forme d'obligation à l'installation ou de discrimination envers les gens qui choisissent de ne pas l'installer.

Les données collectées sont de nature sensible et pourraient être utilisées à **des fins discriminatoires**. Par exemple, un demandeur d'emploi ayant souffert du coronavirus pourrait avoir plus de difficultés à trouver un emploi (par des employeurs "blâmant la victime"). Ces dérives potentielles doivent pouvoir être évitées pour s'assurer que le traitement des données ne génère aucune mesure discriminatoire dans ses différents aspects. L'Organisation Mondiale de la Santé (OMS) met notamment en garde contre la stigmatisation qui pourrait être manifestée à l'égard des personnes atteintes par le virus.

4. Du point de vue politique

Les modalités d'utilisation des données, le contenu des applications et l'étendue des technologies employées doivent être clairement communiquées de façon **transparente**, afin d'être soumis au **regard scrutateur** du grand public et des experts. De même, au vu des nombreuses incertitudes sur l'efficacité des technologies et de l'importance de garantir les principes qui les encadrent, il importe qu'elles soient suivies de près par des instances pluridisciplinaires à même d'évaluer leurs impacts à différents niveaux.

Les mesures exceptionnelles d'emploi des données par le gouvernement (ou une compagnie privée) présentent un risque de **banalisation des mesures de surveillance**. La Pologne a par exemple imposé l'emploi d'une application intrusive aux personnes en quarantaine (GPS activé en permanence, et besoin d'envoyer une selfie de temps à autre sous peine de visite policière). Cela s'est déjà produit aux Etats-Unis, et en Europe, en réponse aux attentats. Sans prise de conscience, l'acceptation des technologies de surveillance par le public, comme une application de traçage de contact ou l'emploi de drones, peut avoir un impact négatif sur notre liberté d'opinion et d'expression.

III. La vision d'AlterNumeris

La crise du Coronavirus est marquée du sceau de l'urgence : urgence sanitaire, économique, sociale et politique. Cette urgence incite les autorités à adopter des mesures fortes, qui risquent de survivre au-delà de la crise elle-même (élaboration d'une base de données des personnes infectées et de leurs contacts ou autre application de traçage des populations et des individus[14], drones de surveillance[15], reconnaissance faciale[16], etc.). Il importe de reconnaître la prudence des autorités[17] ainsi que la participation massive des ONG, des experts et académiques au débat public concernant ces questions complexes et sensibles[18]. Sur le thème du traçage des individus, plusieurs collectifs d'experts ont publié une série de recommandations techniques pour baliser la conception et l'usage de tels systèmes[19] (consentement, limitation dans le temps, architecture de bases de données, etc.).

Si nous soutenons ces propositions et nous rallions aux garde-fous sur lesquelles elles reposent, nous pensons essentiel de se hisser au niveau des politiques du numérique pour envisager la manière avec laquelle le recours aux outils numériques est susceptible d'influencer l'organisation de la vie sociale. La crise sanitaire agit comme une énorme caisse de résonance de notre rapport au numérique. Les réactions face au Coronavirus sont symptomatiques de la manière dont le numérique se glisse dans tous les domaines de nos existences individuelles et collectives ; pris par l'urgence, nous ne sommes pas toujours en mesure de saisir ses impacts sur nos vies et de nos sociétés. En l'absence d'une véritable politique consciente des impacts profonds du numérique, la crise nous plaque contre l'immédiat et nous contraint à agir en étant au pied du mur. Le risque est de perdre de vue la dimension politique des choix posés, de **se voir confisquer le temps de la délibération**, de se laisser capter par les **intérêts de quelques groupes industriels** ou d'abandonner le politique à un solutionnisme techniciste justifié par l'urgence.

Nous considérons que trois enseignements majeurs doivent être tirés de cette crise pour éviter de verser dans ces travers. Ces trois leçons sont de nature à fonder de véritables politiques du numérique qui doivent non seulement nous préparer mieux à affronter les crises futures mais aussi à **renforcer la légitimité démocratique** des choix posés en la matière.

1. Le temps du numérique ne peut pas être celui de l'urgence

En temps de crise sanitaire, l'argument justifiant tous les déploiements technologiques est celui de la sécurité. Nul doute que cette priorité doit peser dans les orientations prises par nos décideurs. Mais l'argument ne peut justifier de couper court à toute réflexion sur les enjeux liés à l'introduction d'une technologie et les alternatives disponibles. Nombre de commentateurs et de citoyens craignent que, comme ce fut le cas pour les attentats terroristes[20], les autorités prennent prétexte de l'urgence pour installer des mesures qui durent bien au-delà de la situation d'urgence. Cette prévalence de l'urgence, en matière de numérique, est également scandée dans les périodes de stabilité ; c'est alors l'urgence économique et les exigences de la compétition internationale qui sont invoquées (le fameux « train du numérique » qu'il ne faut surtout pas rater…).

Dans la crise du Coronavirus, **la question des différentes temporalités en jeu nous semble essentielle**. Différents régimes temporels sont en effet impliqués, qu'il convient de soigneusement démêler. Déplier les différents niveaux de temporalité permet ainsi de poser à chaque fois la question : quelles sont les mesures qui sont temporellement appropriées à la situation ?

On distinguera ainsi, d'une manière générale :

- **La temporalité du *court terme*** lorsqu'il s'agit de prendre des mesures d'application instantanée (confinement, fermetures des commerces, des restaurants, écoles ; commande de matériel, de tests, mesures économiques compensatoires, etc.) ;
- **La temporalité du *moyen terme*** lorsqu'il s'agit de prévoir et organiser le déconfinement, avec toutes ses mesures d'accompagnement à la fois sanitaires, sociales et économiques ;
- **La temporalité du *long terme*** lorsqu'il s'agit de prendre des mesures structurelles contre le retour cyclique du virus, et plus généralement contre de futures pandémies (réforme des systèmes de santé, réorganisation logistique, relocalisation de la production, etc.).
- **La temporalité du *très long terme,*** lorsqu'il s'agit, au-delà des questions spécifiquement sanitaires, d'envisager les impacts sociétaux, voire anthropologiques de dispositifs mis en place à l'occasion de la pandémie (reconnaissance faciale, centralisation des données, etc.).

En matière de numérique, toute décision devrait se prendre à l'aide de lunettes à double focale: une pour la résolution immédiate des problèmes qui surgissent, une autre pour l'impact à long terme des solutions envisagées. Aucune des deux ne peut ni ne doit être envisagée séparément, d'autant plus que l'on connaît l'effet d'engrenage des solutions techniques qui, une fois appliquées, s'avèrent, de fait, irréversibles. La focale du long terme nécessite un passage à la limite : Que se passerait-il si telle solution était généralisée ou si tel dispositif d'exception devenait la norme ? Cette perspective du long terme oblige à réintégrer la technique dans une interrogation politique fondamentale, celle qui donne son sens à toutes les autres : **dans quelle société numérique voulons-nous vivre ?** À cette question, la technique ne peut répondre à notre place ; les techniciens des technologies ne peuvent, seuls, orienter le futur de nos sociétés.

2. Se doter des principes encadrant la conception et l'utilisation d'une technologie … et s'y tenir !

L'emploi du numérique dans cette crise ne doit pas être binaire. Il ne s'agit pas de dire non au numérique, cela serait absolument absurde. Il importe cependant de pouvoir se donner des principes pour orienter leur conception et leur utilisation. Des principes qui, en période de crise comme en période de stabilité, peuvent être mis à mal de multiples manières.

• La nécessité

La nécessité implique que la **technique ne doit être la réponse automatique à tous les problèmes posés**. En effet, d'une manière plus générale, les technologies numériques comblent toujours davantage la passion moderne des puissances publiques et privées pour le contrôle, le calcul, la prévisibilité. D'où un goût apparemment insatiable pour toutes les technologies de prélèvement en continu de données à force de capteurs, de traceurs, et de données personnelles complaisamment offertes au ventre mou des Big Data. C'est ainsi que décisions après décisions, crise après crise, la technologie s'impose comme le cadre par défaut de tous les comportements attendus et des seules solutions envisageables. Cette attitude apparemment neutre est en réalité très idéologique, car elle ne voit de salut que dans la technique, au détriment d'autres possibilités qui ne sont pas même envisagées.

Posons-nous systématiquement la question de la nécessité de l'introduction d'une technologie en **pesant les gains et les pertes qu'elles amènent dans le court et dans le long terme**. La tentation de se tourner automatiquement vers un outil numérique pour résoudre tous nos problèmes, à fortiori en périodes d'instabilité, doit être contenue et soumise à la réflexion.

• L'évaluation préalable et continue du système numérique utilisé

Il nous semble essentiel de prévoir les conditions de l'expérimentation avant de généraliser un usage à toute une population. De même, il importe de pouvoir garantir le contrôle de son utilisation et de réaliser l'évaluation de ses effets à long terme.

EXEMPLE 1 : Nécessité et évaluation d'une application de traçage de la population

Le traçage de la population via une application installée sur nos téléphones 'intelligents' a été déployé dans plusieurs pays, offrant à la Belgique suffisamment de recul pour évaluer préalablement les effets de ce système. Dans les faits, le faible taux d'adoption de l'application par les populations[21], les risques élevés de faux-positifs[22] ainsi que la faible valeur ajoutée de l'application[23],[24] peut légitimement remettre en cause la nécessité d'un tel système. Celui-ci s'avérerait même contre-productif s'il donnait un faux sentiment de sécurité à la population[25]. Puisque ce système semble toutefois être bientôt déployé en Belgique, l'évaluation continue de son efficacité et de sa plus-value (via des résultats quantifiés) est indispensable. Notons qu'une telle évaluation n'est pas prévue puisque seule l'évaluation sur le fonctionnement de l'application est envisagée dans les textes juridiques actuels, afin de régler les problèmes qui seront décelés au fil du temps (de sécurité, de vie privée ou de fonctionnalité) et qui sont inhérents au développement d'une telle application, comme cela a pu être observé notamment chez nos voisins français[26] ou allemands[27].

• La proportionnalité

La proportionnalité, à savoir l'adéquation entre les mesures prises et la finalité poursuivie, minimise le volume des données collectées et garantit l'anonymat. Les autorités belges et françaises en matière de vie privée précisent également - dans le cas particulier du traçage - qu'il faut démontrer que la solution utilisée (technologique ou pas) est le moyen le moins intrusif pour atteindre l'objectif poursuivi.

Il y de quoi s'alarmer lorsque des entreprises surenchérissent sur les mesures de surveillance en installant à leurs portes des dispositifs de bracelets électroniques[28] ou de reconnaissance

faciale sous prétexte de sécurité sanitaire[29,30]. A la côte belge, un réseau de 250 caméras intelligentes est prévu pour gérer l'afflux de touristes[31] **L'urgence déborde ici la temporalité du droit**. Tout ce déploiement numérique est-il approprié, proportionné ? Le gain immédiat apparent n'est-il pas surclassé par les effets au long cours ?

EXEMPLE 2 : Régulation du flux de clients dans les magasins via reconnaissance faciale

En Belgique, une start-up propose d'installer des caméras à l'entrée des magasins afin de pouvoir compter les personnes et donc s'assurer que les règles de sécurité sanitaires soient bien respectées (nombre de personnes par m²), mais aussi de filtrer les clients à l'entrée en mesurant leur température[32]. Premièrement, on peut questionner la nécessité de la mesure de température. L'Autorité de Protection des Données mentionne clairement que ces pratiques ne sont pour le moment pas autorisées et rappelle également l'inefficacité partielle d'un tel système dans la lutte contre la propagation du COVID-19[33]. Ensuite, on peut questionner la proportionnalité du système de caméra ici mis en œuvre pour compter les clients, sachant que d'autres systèmes simples (vigile à l'entrée, compteur laser…) peuvent remplir le même objectif de façon nettement moins intrusive. Dans la presse, cette startup annonce que son système de surveillance va évoluer dans le temps et s'enrichir d'autres options[34] (profil et comportements des clients, etc.), ce qui questionne également sur la temporalité et la finalité réelle d'un tel système.

EXEMPLE 3 : Banque de données pour lutter contre la propagation du COVID-19

Fin mai, une proposition de Loi sur la création d'une banque de donnée gérée par Sciensano est déposée. A deux reprises, l'Autorité de Protection des Données a jugé la proposition illégale au regard du RGPD - le texte ne démontrant pas le caractère nécessaire et proportionnel de la collecte et de l'enregistrement de toutes les données, ce qui est pourtant requis[35]. Un autre grief majeur émis dans cet avis est la violation du secret médical.

• Transparence technique

La transparence technique concerne la conception et le code de l'application, y compris leurs auteurs, la finalité de l'application ainsi que l'exploitation des données qu'elle collecte, afin que chacun puisse être assuré qu'elle ne fait que ce qu'elle est censée faire.

EXEMPLE 4 : Transparence technique et code source

En informatique, le code source est un texte qui présente les instructions composant un programme sous une forme lisible, telles qu'elles ont été écrites dans un langage de programmation. Ainsi, la publication du code source des applications de traçage est une condition élémentaire de transparence. Certains pays comme la France [36], Grande-Bretagne[37] et l'Inde[38] ont déjà embrayé dans ce sens ; la Belgique devrait en faire autant avec Coronalert. Notons toutefois que Coronalert se base sur le « Exposure Notification System » d'Apple/Google et que ce système, contenant l'essentiel du protocole de traçage, n'est que partiellement public. Il reste donc une bonne part de confiance aveugle à faire à ces deux géants américains du numérique. Si la publication du code semble être sur la bonne voie dans les applications de traçage, on notera que c'est loin d'être le cas pour d'autres applications de type *reconnaissance faciale* - où le code source est la plupart du temps la propriété des entreprises qui les développent.

• Transparence politique

La transparence politique a trait aux conditions dans lesquelles les décisions sont prises en matière de politique numérique.

EXEMPLE 5 : Transparence politique de la Taskforce "Data Against Corona"

C'est à la suite d'une carte blanche[39] d'entrepreneurs *tech* dans la presse francophone qu'un groupe de travail "Data & Technology Against Corona" a été créé par le ministère de la santé et celui en charge du numérique[40], afin d'aider le gouvernement à prendre de bonnes décisions en matière d'utilisation des données et des technologies. Le fonctionnement de ce groupe de travail reste opaque, la liste de ses membres ainsi que les rapports des travaux réalisés n'étant officiellement publiés nulle part[41].

3. Une politique du numérique : Connecter technologie et société

Afin d'éviter une mécanique du fait accompli, nous défendons la nécessité d'une réflexion commune et transparente sur les usages, implications et potentialités des outils numériques. Seule une telle réflexion permettra d'affronter cette crise et celles qui suivront dans une forme de maturité démocratique, qui semble faire défaut aujourd'hui. **Une politique du numérique forte doit pouvoir s'appuyer sur toutes les voix qui comptent dans le débat public** ainsi que sur les mécanismes démocratiques existants.

Ce n'est qu'en se réappropriant démocratiquement et structurellement les outils numériques et le système qui les sous-tend que nous pourrons nous approprier en confiance le sens du progrès technologique. Permettre cette réappropriation, c'est nous permettre de devenir des sujets *politiques* du numérique, pour l'habiter autrement que sur le mode du fait accompli, en temps de crise comme en tout autre temps. Nous appelons à faire advenir une politique du numérique en développant l'interface entre technologie et société.

Concrètement, que faire ?

Se doter des moyens institutionnels

Durant cette crise, des propositions ont émergés dans le sens d'une présence plus importante de citoyens au sein des comités d'expert ou, dans le cadre du projet spécifique de mise en place d'une application de traçage, la constitution d'un comité de suivi permettant de s'assurer que l'ensemble des principes guidant une utilisation responsable du numérique puissent être respectés.

A la lumière de ces enseignements, nous insistons sur les traits structurels qui doivent gouverner une politique du numérique authentiquement démocratique. Pour rendre les citoyens non seulement **conscients des enjeux mais aussi acteurs des décisions à prendre**, nous avons besoin d'outils démocratiques adéquats et durables, de formes institutionnelles appropriées. C'est pourquoi, parmi nos propositions, se trouve notamment la **constitution d'un institut pluridisciplinaire et indépendant** chargé de faciliter le débat public autour de ces sujets, d'informer les décisions publiques et de soutenir les processus de participation citoyenne en matière technologique. Il s'agirait d'élaborer de nouvelles interfaces entre technologies et société, d'inventer de nouveaux processus de débats démocratiques, et d'articuler les progrès technologiques aux exigences d'une société *désirable*.

Collaborer avec AlterNumeris

Le collectif AlterNumeris se tient à disposition des citoyens, des formateurs, décideurs politiques ainsi que de la société civile, afin d'aider, d'accompagner, de conseiller toute initiative ayant pour objectif de développer la démocratie numérique ou de cultiver la citoyenneté numérique.

https://www.alternumeris.org/

CONTACT: STEVE TUMSON · 0494 932 313 · INFO@ALTERNUMERIS.ORG

Références

1 L'Echo, Utilisons les données télécom de tous les Belges pour stopper le coronavirus

2 RTBF, Des « données contre le Corona » : votre téléphone peut lutter contre le virus

3 RTBF, L'analyse des déplacements, via GSM, a influencé les décisions du Conseil National de Sécurité

4 Le Soir, Coronavirus: quid d'une appli de traçage belge?

5 De Standaard, De Backer: 'Voor contactonderzoek is eigenlijk geen app nodig'

6 RTBF, Le traçage via téléphone portable a du plomb dans l'aile

7 RTBF, Une app pour tracer les porteurs du coronavirus ? L'APD demande au fédéral de revoir sa copie

8 L'Avenir, Application anti-coronavirus: un travail dans le désordre

9 RTBF, Coronavirus : la Belgique mise sur l'application de tracing début juillet

10 RTBF, Coronavirus en Wallonie : le nombre de "contact tracers" va être réduit, faute d'appels à traiter

11 RTBF, Lutte contre le coronavirus en Belgique : que prévoit l'accord de coopération sur le traçage?

12 Le Vif, Les coulisses de la saga Coronalert (...)

13 > https://www.autoriteprotectiondonnees.be/avis-de-lautorite
> http://www.raadvst-consetat.be/

14 RTBF, Coronavirus en Belgique : le parlement veut encadrer une future application de tracking

15 RTBF, Des parcs bruxellois encore très fréquentés, la police déploie ses drones

16 RTBF, Déconfinement : comment l'intelligence artificielle régule le trafic clients en magasin

17 Site de l'Autorité de Protection des Données (APD), Applications de traçage et base de données COVID-19: pour l'APD, les avant-projets d'arrêtés royaux doivent être revus

18 Le Soir, L'efficacité du traçage se heurte à la protection de la vie privée

19 > Collectif de 600 scientifiques internationaux : Déclaration commune sur le traçage des contacts

> Collectif de 123 académiques belges (p59-62) : Stratégie de déconfinement
> Membres de l'Académie Royale des Sciences de Belgique, «Tracing: attention aux exploitations non désirables de nos données!»

20 Rapport de recherche du CREDOF, Ce qui reste(ra) toujours de l'urgence

21 MIT Tech Review initiative, Covid Tracing Tracker

22 Dossier du CNRS, Risques et limites des applications de traçage

23 Technology Review, Nearly 40% of Icelanders are using a covid app—and it hasn't helped much

24 The Guardian, How did the Covidsafe app go from being vital to almost irrelevant?

25 La Tribune Toulouse, "StopCovid risque de donner un faux sentiment de sécurité" (Baptiste Robert)

26 Site de la CNIL, Application StopCovid : la CNIL tire les cons_equences de ses contrôles.

27 Il y 77 bugs ouverts répertoriés sur Github, pour la version Android, au 12/9/20 : https://github.com/corona-warn-app/cwa-app-android/issues

28 RTBF, Un bracelet intelligent renseignant la distance sociale en test dans le port d'Anvers

29 NouvelObs, Des caméras intelligentes pour surveiller le port du masque dans le métro parisien (...)

30 Libération, A Cannes, des caméras scrutent les habitants non masqués

31 Le Soir, Déconfinement: 250 caméras intelligentes surveilleront les touristes à la Côte

32 Le Soir, Une startup automatise le comptage des clients dans les magasins

33 Avis de l'ADP, Prise de température dans le cadre de la lutte contre le COVID-19

34 UCM Magazine, La créativité et le rebond des PME

35 Avis n°42 APD, p10, Demande d'avis concernant une proposition de loi de loi portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du COVID-19

36 Tom's Guide.fr, StopCovid : le gouvernement met à disposition le code source de l'application

37 BBC, Coronavirus: NHS reveals source code behind contact-tracing app

38 Tech Crunch, India's contact-tracing app is going open-source

39 L'Echo, "Utilisons les données télécom de tous les Belges pour stopper le coronavirus"

40 Digimedia.be, Une « Data Against Corona Taskforce » pour analyser les informations sur la propagation du Covid-19

41 E-ealth.fgov.be, Le rôle de la Task Force 'Data & Technology against Corona'