Le traçage numérique est-il nécessaire dans une société démocratique ?

Degrave, Elise

Published in:
Des enjeux d'intérêts public en temps de pandémie

Publication date:
2021

Document Version
le PDF de l'éditeur

LE TRAÇAGE NUMÉRIQUE DES CITOYENS EST-IL NÉCESSAIRE DANS UNE SOCIÉTÉ DÉMOCRATIQUE ?

Élise Degrave
Professeure à la Faculté de droit de l'Université de Namur
Directrice de recherche au Namur Digital Institute/CRIDS
Codirectrice de la Chaire Egov de l'Université de Namur

Lutter contre la propagation du coronavirus exige-t-il de recourir au traçage numérique des citoyens ? La question fait débat dans de nombreux États[1]. Il s'agit de proposer aux citoyens de télécharger une application sur leur smartphone qui enregistre les personnes avec qui ils sont en contact. Si la personne ayant téléchargé l'application est testée positive, les personnes de contact seront averties du risque d'avoir été contaminées et encouragées à s'isoler et se faire tester.

L'idée est séduisante. Dans la peur et l'urgence, nous aimerions tant que la technologie soit la baguette magique pour nous sortir de là[2].

Malheureusement il n'en n'est rien. La technologie n'est qu'un moyen au service d'un projet de société. Un moyen qui n'est pas anodin, car les choix technologiques faits aujourd'hui dessinent les contours de la société de demain. C'est pourquoi, il est de la responsabilité des États de soumettre de tels choix à un débat démocratique éclairé et éclairant, avant de les proposer à toute une population, pour s'assurer que ce qui est technologiquement faisable, est également démocratiquement acceptable.

Cette démarche de dialogue, de pédagogie et de transparence est d'autant plus importante que le traçage numérique des citoyens touche à la gestion des données par l'État, qui se rattache au domaine de l'« e-gouvernement », particulièrement mis en lumière par la crise du Covid. Certes les citoyens communiquent déjà nombre de leurs informations aux GAFAM[3], et l'on pourrait croire ainsi que la circulation des données se banalise. Mais cette image d'Épinal ne doit pas faire oublier que les données confiées à l'État sont

1. Dans les lignes qui suivent, nous limitons nos réflexions au cadre juridique européen (Union européenne et Conseil de l'Europe).
2. C'est ce que l'on appelle traditionnellement « le solutionnisme technologique ».
3. Acronyme de Google, Apple, Facebook, Amazon et Microsoft, entreprises qualifiées de « géants du net ».

précieuses, et soulèvent des enjeux très particuliers. En effet, à la différence de sa relation avec Google ou Facebook, le citoyen ne peut se passer de l'État et ne peut pas non plus lui mentir. Il est obligé, dès sa naissance, de lui confier de très nombreuses données, fiables, qui concernent toutes les facettes de sa vie (des données fiscales, sociales, cadastrales, familiales, de santé,...). Par ailleurs, à la différence des GAFAM, l'État a des pouvoirs importants et bien à lui, notamment en termes de contrôle et de surveillance des citoyens, puisqu'il a notamment le monopole de la contrainte.

Jusqu'à présent, le citoyen collabore à ce mode de fonctionnement car il y a un pacte de confiance entre lui et l'État qui suppose que ce dernier soit loyal et transparent. En principe d'ailleurs, ce pacte est ancré dans des normes censées encadrer minutieusement la gestion des données des individus par la puissance publique.

Mais, aujourd'hui, ce pacte est-il encore respecté ? Les nombreuses zones d'ombre qui entourent le traçage numérique, pourtant déjà effectif dans plusieurs États, sèment le doute. Les premiers retours d'expérience semblent d'ailleurs révéler que le manque de confiance en l'État a un impact sur le taux de téléchargement des applications de traçage. Puisque, cette fois, le citoyen a le choix de télécharger ou non cet outil, lorsque sa confiance est lézardée par la suspicion, il réfléchit à deux fois avant de communiquer de nouvelles données aux institutions publiques. La confiance en l'État est d'ailleurs une explication avancée pour expliquer le succès plus important de l'application de traçage allemande par rapport à l'application française, par exemple[4].

Certes, il n'est pas certain que la technologie, et cette nouvelle collecte de données organisée par l'État, soit liberticide. Il n'est pas non plus certain qu'elle ne le soit pas. Dans la peur et l'urgence, doit-on fermer les yeux sur les risques du traçage numérique pour les libertés, et pour la vie privée en particulier ? Ne serait-il pas plus sage, et efficace, de privilégier à tout prix la santé, le temps que s'éteigne la crise ? Ce serait oublier l'effet « cliquet » des droits fondamentaux : une liberté perdue un jour l'est pour toujours[5]. En l'occurrence, veiller à maintenir vivaces tant la santé que la vie privée, et, de manière générale, l'ensemble des libertés, c'est se préserver, plus tard, des effets secondaires de la crise, sur le plan sanitaire mais aussi démocratique.

Après avoir délimité le cadre juridique de référence du traçage numérique, la présente étude analyse la nécessité du traçage numérique, en particulier au regard des risques que cette technologie peut générer.

I. LE CADRE JURIDIQUE DE RÉFÉRENCE

A. – Le Règlement général pour la protection des données

Le traçage numérique des citoyens suppose l'utilisation des données à caractère personnel de ceux-ci. En effet, cette pratique doit permettre de retrouver les personnes de contact pour les prévenir d'une possible contamination. Il est donc nécessaire de recourir à des données permettant d'identifier ces personnes. De ce fait, le traçage numérique doit respecter le Règlement général sur la protection des données à caractère personnel (ci-après « RGPD »)[6].

Pour cette raison, depuis le début de la pandémie, plusieurs institutions nationales et supranationales œuvrant à la protection des données ont publié des documents reprenant les exigences juridiques du RGPD qui s'imposent aux applications de traçage. Parmi celles-ci figurent la détermination claire des finalités de l'application[7], la minimisation des données collectées[8], l'identification du responsable du traitement de l'application[9], etc.

Le réflexe de se plonger dans le RGPD dès qu'il est question de traiter des données à caractère personnel ne doit pas éclipser le fait que le RGPD n'est qu'un ensemble d'instructions, un « mode d'emploi », qu'il y a lieu de suivre pour construire un traitement de données respectueux de certaines garanties juridiques. Mais la protection des données organisée par le RGPD n'est pas une valeur en elle-même. L'équilibre que tentent d'instaurer ces règles de protection

4. À ce sujet, v. not. https://www.lesnumeriques.com/telephone-portable/pourquoi-l-application-de-tracage-numerique-allemande-connait-elle-deja-un-meilleur-demarrage-que-stopcovid-n151567.html Une spécialiste de l'Allemagne y explique notamment que *« la constitution allemande est faite par contraste avec son histoire. Tout est fait pour qu'il y ait débat collectif et décisions collectives. D'ailleurs, si l'application était centralisée et intrusive, il y aurait une saisine immédiate de la Cour constitutionnelle de Karlsruhe, qui est une institution puissante »*. Des chercheurs de l'Université d'Oxford ont consacré une étude à l'« acceptabilité d'une application téléphone pour tracer les contacts porteurs du Covid-19 » en juin 2020. Elle est accessible ici https://osf.io/24uan/

5. À l'expression traditionnelle « effet cliquet », on préfère toutefois la métaphore, moins sérieuse mais plus percutante, selon laquelle « les libertés, c'est comme du dentifrice : quand ça sort du tube, ça n'y rentre plus jamais »...

6. Le RGPD s'applique à tous les traitements de données à caractère personnel, tels que définis au Chapitre I du RGPD.

7. Les applications de traçage peuvent poursuivre différentes finalités comme le suivi des contacts, l'auto-diagnostic, le contrôle du confinement, etc. V. Conseil de l'Europe, *Solutions numériques pour lutter contre la Covid-19,* oct. 2020, préc., p. 33-34.

8. L'application peut collecter certains identifiants mais pas l'état civil de la personne, par exemple. V. not. European Data Protection Board, *Lignes directrices 4 /2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de Covid-19,* 21 avr. 2020, préc., n° 41.

9. En France, le responsable du traitement pour l'application *TousAntiCovid* est la Direction générale de la santé du ministère des Solidarités et de la Santé. V. https://bonjour.tousanticovid.gouv.fr/privacy.html

des données, entre le responsable du traitement et la personne dont les données sont traitées, n'existe pas dans l'absolu. Cet équilibre doit être défini par rapport à un idéal à atteindre et en fonction d'un contexte particulier.

C'est pour cette raison que la protection des données à caractère personnel s'enracine dans une valeur fondamentale, la vie privée, consacrée par l'article 8 de la Convention européenne des droits de l'homme[10].

B. – La Convention européenne des droits de l'homme (ci-après « Conv. EDH »)

L'article 8 Conv. EDH, dédié à la protection de la vie privée, consacre un droit particulièrement riche, pour plusieurs raisons. Nous en soulignons deux.

D'une part, la vie privée est le socle des autres libertés. Si la vie privée est malmenée, notamment par des abus dans l'usage des données à caractère personnel, d'autres droits fondamentaux seront menacés. Ainsi, en balisant l'usage des données de santé relatives au Covid, on protège le droit à l'égalité et à la non-discrimination. En encadrant l'utilisation des données relatives aux contacts des citoyens, on veille à protéger la liberté d'association et la liberté d'aller et venir.

D'autre part, à l'heure du numérique, le droit à la vie privée ne se limite pas à la protection de l'intimité. Ce droit s'interprète comme le droit à l'autodétermination informationnelle, c'est-à-dire le droit de tout individu de maîtriser son image informationnelle, en décidant lui-même des conditions d'utilisation de celle-ci ou, au moins[11], en ayant connaissance de l'usage qui en est fait, par exemple en recevant des explications sur la réutilisation des données Covid par l'État.

Ainsi portée vers l'idéal de la vie privée, la protection des données incarne les conditions nécessaires au développement libre de chaque personne, inspirées de solitude et de participation. Charles Fried ne disait pas autre chose lorsqu'en 1968 déjà, il affirmait que « to respect, love, trust, feel affection for others and to regard ourselves as the objects of love, trust and affection is at the heart of our motion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion »[12].

Ainsi donc, le traçage numérique doit, certes, respecter les exigences du RGPD. Mais, avant cela, la valeur de la vie privée, qu'incarne l'article 8 Conv. EDH, doit

10. À ce sujet, v. E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* Bruxelles, Larcier, coll. du CRIDS, 2014, n° 60 et s.

11. Cette nuance est liée au fait que, dans l'e-gouvernement notamment, il y a des situations dans lesquelles le citoyen est obligé de donner ses informations personnelles. C'est le cas, par exemple, des données du Registre national qui sont obligatoirement enregistrées, à défaut de quoi le citoyen n'aurait pas d'existence civile.

12. C. Fried, « Privacy », *Yale Law Journal* 1968, vol. 77, p. 477 et p. 478.

constituer le socle de la réflexion. En particulier, la question de la nécessité du traçage numérique nous est (im)posée par l'article 8 Conv. EDH.

II. L'ARTICLE 8, § 2, CONV. EDH ET LA NÉCESSITÉ DU TRAÇAGE NUMÉRIQUE

A. – « Nécessaire dans une société démocratique »

En ce qu'il mobilise des traitements de données à caractère personnel, le traçage numérique est une ingérence dans la protection de la vie privée des citoyens[13]. Aux termes de l'article 8, § 2, Conv. EDH, une telle ingérence doit être « nécessaire dans une société démocratique ».

La Cour européenne des droits de l'homme rappelle régulièrement que le droit à la vie privée n'est pas absolu et qu'une ingérence est possible si la norme, rédigée de manière claire et prévisible, répond à un besoin social impérieux et organise une ingérence proportionnée dans la vie privée[14].

En l'occurrence, force est de reconnaître que la lutte contre la pandémie est un « besoin social impérieux ». Mais le traçage numérique est-il une mesure proportionnée à cet objectif ? Il s'agit là d'une question délicate « car marquée, inévitablement, par l'imprévisibilité et donc l'insécurité »[15] propres au contrôle de la proportionnalité de la mesure.

Avant d'étudier le contrôle de proportionnalité comme tel, les lignes qui suivent abordent deux particularités de la régulation du traçage numérique, à savoir la menace de la technocratie et l'illusion de la base volontaire de téléchargement.

B. – Technicité et technocratie

Évaluer la nécessité d'une technologie n'est pas une chose évidente, surtout s'agissant des applications de traçage à propos desquelles nous n'avons pas encore de

13. V. not. Cour EDH, 16 févr. 2000, *Amann c. Suisse,* n° 27798/95, § 65. Remarquons également qu'un outil informatique « constitue une intrusion corrélativement plus importante dans les droits (...) au respect de la vie privée et à la protection des données à caractère personnel » que les outils traditionnels [conclusions de l'avocat général E. Sharpston, du 17 juin 2010, § 96, sous CJUE, Gde ch., 9 nov. 2010, *Volker und Markus Schecke et Eifert GbR et Hartmut Eifert,* aff. jointes C-92/09 et C-93/09. Pour plus de détails, v. E. Degrave, *L'e-gouvernement et la protection de la vie privée, op. cit.,* n° 59 et s.

14. En matière de protection des données, v. not. Cour EDH, 4 mai 2000, *Rotaru c. Roumanie,* n° 28341/95, § 43, qui est un arrêt fondateur en la matière. À ce sujet, v. E. Degrave, *L'e-gouvernement et la protection de la vie privée, op. cit.,* n° 103 et s.

15. B. Renauld et S. Van Drooghenbroeck, « Le principe d'égalité et de non-discrimination », *in* M. Verdussen et N. Bonbled (dir.), *Les droits constitutionnels en Belgique,* Bruxelles, Bruylant, 2011, vol. 2, p. 593.

réel recul. Cela suppose notamment que l'on soit éclairé sur son efficacité, et donc sur son fonctionnement. Surgissent alors des questions complexes, faisant appel à des connaissances techniques parfois poussées ainsi qu'à un vocable particulier, fait d'abréviations étranges et de concepts inédits par rapport auxquels le droit est peu familier. Ces difficultés peuvent donner un aspect très obscur aux questions juridiques discutées. Face à de telles questions, les parlementaires et les ministres concernés préfèrent souvent en appeler à des experts. Ces derniers rédigeront, dans l'ombre, le projet de loi. Le ministre concerné, faisant aveu de sa méconnaissance du dossier, l'approuvera, tandis que les débats au Parlement pâtiront de leur technicité et pourraient souffrir d'un manque d'intérêt de la part des représentants du peuple.

Ces dérives ne sont pas propres à l'encadrement des technologies, mais elles se révèlent ici avec une acuité particulière. Elles doivent retenir notre attention parce que, bien que ces experts ne soient pas nécessairement malveillants, on ignore qui ils sont, on ne peut garantir leur indépendance politique ou économique, et ils n'ont aucune responsabilité politique. En outre, ils sont chargés de rendre l'outil fonctionnel, et auront donc à cœur d'être efficaces et rationnels au risque, peut-être, de négliger la protection des libertés citoyennes. En d'autres termes, « derrière une scène politique offerte au regard de tous, (...) on découvre la réalité cachée de l'administration technicienne pour qui la poursuite de l'efficacité passe avant toute autre considération. C'est dans la recherche d'une plus grande rationalité technique qu'elle trouve la justification de la clandestinité de son action et le moyen d'imposer ses vues »[16]. Ce faisant, l'Homme, et avec lui, ses idéaux, ses convictions politiques, son vécu psychologique, risquent d'être considérés comme le principal obstacle de cette révolution technologique et des choix mathématiques qui l'accompagnent.

Cela peut se traduire par une domination progressive de la technique sur le droit[17], face à laquelle on ne peut se résigner. Ce risque de technocratie une fois identifié, il doit stimuler encore davantage les débats démocratiques approfondis, publics et transparents, dans ce domaine, pour que ce soit la loi qui encadre la technologie et non la technologie qui fasse loi.

C. – Le téléchargement sur une base volontaire illusoire

Les applications de traçage européennes sont proposées aux citoyens « sur base volontaire »[18]. Libre à chacun de décider s'il télécharge, ou non, cette application.

16. A. Vitalis, *Informatique, Pouvoir et Libertés*, 2e éd., Paris, Economica, 1988, p. 107.
17. À cet égard, comme l'affirme le professeur Xavier Philippe, « plus la technologie est avancée, plus elle est difficile à comprendre moins on la comprend plus le droit perd son emprise et son pouvoir protecteur ». Séminaire « Le traçage numérique : un pacte avec le diable ? », Discussion entre les membres de l'ISJPS à la suite du séminaire proposé par Élise Degrave et Judith Rochfeld, 3 juin 2021, à partir de 15 :50, accessible ici https://mediatheque.univ-paris1.fr/video/2516-le-tracage-numerique-un-pacte-avec-le-diable/
18. V. Conseil de l'Europe, *Solutions numériques pour lutter contre la Covid-19*, oct. 2020, préc., p. 11.

Pourtant, si l'efficacité du traçage numérique demeure incertaine, les risques, notamment techniques, sont bien réels, ainsi qu'on l'analysera dans la suite de cette étude. Ce constat sème le doute sur la nécessité de cet outil. Dans ce contexte, n'est-ce pas malaisant de proposer une application de traçage « sur base volontaire », caractéristique d'ailleurs largement mise en avant dans les diverses communications publiques à ce sujet ? N'est-ce pas là, pour l'État, une manière d'esquiver le test de nécessité jugé trop délicat et de faire peser, sur le citoyen, une partie de l'incertitude entourant les avantages et les risques de cette application ?

On peut raisonnablement se poser la question en constatant que les États européens – même eux – pourraient rendre le traçage numérique obligatoire. En effet, le RGPD autorise les États à imposer un traitement, tel qu'une application de traçage, lorsqu'il est « nécessaire à la sauvegarde des intérêts vitaux »[19] des personnes ou pour lutter contre « les menaces transfrontalières graves pesant sur la santé »[20].

En définitive, l'État étant convaincu qu'il est nécessaire, pour limiter la vitesse automobile et diminuer le nombre d'accidents de la route, de placer des radars qui enregistrent les plaques d'immatriculation, il ne laisse pas le choix au citoyen d'accepter, ou non, ces dispositifs de contrôle. Il est piquant de se demander pourquoi, alors, ne pas faire de même avec l'application de traçage, si, aux yeux des États, elle est incontournable pour lutter contre la pandémie[21]. La question se pose d'autant plus qu'imposer à tous l'utilisation de cette application contribuerait à son efficacité[22].

On peut ainsi être tenté de se dire que l'État, n'étant pas vraiment convaincu par la nécessité de cette application, laisse le citoyen effectuer lui-même l'examen de proportionnalité entre les avantages et les inconvénients de l'appli. En cas de problèmes ultérieurs, les reproches adressés à l'État seront moindres puisque le citoyen était libre de recourir, ou non, à cette application.

Cette question est d'ailleurs clairement posée et analysée par l'Observatoire international sur les impacts sociétaux de l'IA et du numérique au Québec, qui conclut que « dans le contexte actuel, il serait probablement difficile pour le gouvernement de faire la démonstration que l'obligation d'installer une application de notifications d'exposition est une mesure qui est raisonnable en regard du droit québécois et canadien. C'est probablement pourquoi les gouvernements ont souvent répété que l'adhésion à de telles applications demeurerait volontaire »[23].

19. Art. 6, 1., d) RGPD.
20. Art. 9, 2., i) RGPD. L'association de Max Schrems, qui milite pour la protection des données, a mis ce point en avant soutenant que « la question n'est pas "si" mais "comment" ». V. https://noyb.eu/en/data-protection-times-corona
21. En ce sens, v. notamment les propos d'un chercheur français appelant à recourir au traçage obligatoire selon le modèle coréen https://amp.lepoint.fr/2373847?
22. V. *infra*.
23. https://observatoire-ia.ulaval.ca/qa_covid/

À notre sens, ce caractère volontaire du téléchargement de l'application est illusoire. Le citoyen est démuni par rapport aux questions qu'il doit se poser. On exige de lui qu'il fasse lui-même l'examen délicat et difficile de la nécessité de cette application, et notamment de ses risques. Or ce ne peut lui être demandé tant le sujet est complexe et les enjeux importants[24].

Par ailleurs, chacun peut être influencé, voire mis sous pression[25]. De nombreuses publicités pétillantes et colorées incitent à télécharger l'application, celle-ci est proposée par l'État qui en encourage lui-même le téléchargement, le qualifiant de « geste citoyen »[26]. Au-delà, la peur du virus convainc de recourir à tout ce qui semble être une solution pour sortir de la crise[27], sans parler de la pression sociale qui invoque la solidarité entre citoyens. Les plus grands doutes entourent donc la réalité de ce consentement, qui ne devrait intervenir qu'en tant que modalité supplémentaire, une fois qu'il est tout à fait certain que l'État peut assumer la mise en place de tels traitements avec autant de certitude que s'il l'imposait à toute la population. À l'heure actuelle, cette certitude est illusoire.

D. – Le contrôle de la proportionnalité du traçage numérique

Le contrôle de la proportionnalité du traçage numérique est à plus forte raison délicat qu'il est bardé d'incertitude, notamment technique, d'autant plus que, comme nous l'avons souligné précédemment, ces applications sont nouvelles et que nous n'avons pas de recul à leur égard.

Tant la Commission nationale informatique et libertés (« CNIL ») que l'Autorité de protection des données belge (« APD »), pour ne citer qu'elles, se sont prononcées sur la proportionnalité des applications de traçage numérique concernant leur territoire national. Leurs analyses divergent.

24. À cet égard, v. l'exemple de pédagogie réalisé par l'Observatoire international sur les impacts sociétaux de l'IA et du numérique, et son « petit guide sur les enjeux et opportunités des applications de notifications d'exposition à la Covid-19 », en particulier la rubrique 10 « Avant d'installer une telle application, quelles questions dois-je me poser » https://observatoire-ia.ulaval.ca/qa_covid/

25. Par ex., mi-octobre, soit plus d'un mois après l'entrée en application de « Coronalert », le Comité interfédéral chargé du traçage et des tests assénait « *Cette application est l'un des outils mis en place pour lutter contre la Covid-19, alors invitez vos amis et votre famille à télécharger Coronalert* » (https://www.rtbf.be/info/societe/detail_coronavirus-l-application-coronalert-telechargee-par-un-million-de-belges?id=10607469).

26. Expression entendue dans une communication radio en Belgique.

27. En Belgique, c'est l'apparition de la deuxième vague, mi-septembre 2020, qui a surtout convaincu les citoyens de télécharger l'application coronalert.

La CNIL, se prononçant sur un projet de décret, donne un feu vert à « Stopcovid », constatant « l'utilité de l'application »[28] conjuguée à certaines garanties telles que « le volontariat des utilisateurs »[29] et le respect des balises exigées par le RGPD[30].

L'Autorité de protection des données belge chargée elle aussi de se prononcer sur un projet du gouvernement, est plus sévère dans son analyse. Elle procède à un « test de proportionnalité fort »[31], en rappelant que « toute ingérence dans le droit au respect de la vie privée, en particulier lorsque l'ingérence s'avère importante, n'est admissible que si elle est nécessaire et proportionnée à l'objectif d'intérêt général qu'elle poursuit »[32].

S'agissant de l'examen de la *nécessité* de l'application de traçage, l'APD se penche sur son efficacité et estime que celle-ci n'est pas suffisamment démontrée. Ce faisant, très judicieusement, l'APD ne prend pas pour acquis que le numérique permet nécessairement de sortir de la crise, et exige du gouvernement qu'il apporte lui-même la preuve de la nécessité de l'outil qu'il veut mettre en place, et pas seulement la preuve que cet outil respecte le RGPD. C'est pourquoi, l'APD réclame « une estimation du pourcentage de la population qui en fera usage, sur la base de sondages récents d'intention », ainsi qu'« une étude relative au taux d'utilisation requis pour que le système produise des résultats »[33]. Cette demande renvoie au fait que les applications de traçage ne fonctionnent qu'à la condition d'être massivement téléchargées par la population, par au moins 60 % de la population[34]. Notons que, depuis lors, ce pourcentage n'a pas été atteint dans les États concernés. À titre d'exemple,

28. CNIL, délibération n° 2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid », not. n° 13 et n° 20.

29. *Ibid.*, n° 27 et s.

30. Pour plus d'informations sur Stopcovid et une comparaison avec plusieurs États européens et non européens, v. S. Peyrou-Bartoll, « Covid-19 et droits fondamentaux : la protection des données à caractère personnel à l'épreuve de la pandémie », *RAE/LEA* 2020/1, p. 53 et s.

31. À ce sujet, v. R. Gellert et S. Gutwirth, « The legal construction of privacy and data protection », *Computer Law & Security Review* 2013, p. 522-530, accessible ici https://www.sciencedirect.com/science/article/pii/S0267364913001325

32. Autorité de protection des données, avis n° 34/2020 concernant un avant-projet d'arrêté royal (…) dans le cadre de l'utilisation d'applications numériques de dépistage de contacts par mesure de prévention contre la propagation du coronavirus Covid-19 parmi la population, n° 6.

33. APD, avis n° 34/2020, n° 9.

34. Observatoire international sur les impacts sociétaux de l'IA et du numérique (Canada), *Efficacité et enjeux sociétaux des apps de traçage de contacts,* 27 avr. 2020, accessible ici : https://observatoire-ia.ulaval.ca/3674/. À propos de l'acceptabilité sociale des applications de traçage, des chercheurs de l'Université d'Oxford ont mené une étude au mois de mars 2020, en France, en Allemagne, au Royaume-Uni, en Italie et aux États-Unis. Cette étude est accessible ici : https://osf.io/24uan/

« Stopcovid » a été téléchargée par 4,5 % des Français[35]. « Coronalert » a été téléchargée par 15 % des Belges[36] mais requiert, pour son efficacité, que les personnes testées positives demandent à l'application de prévenir les personnes de contact, ce qu'elles ne font pas pour la plupart d'entre elles. Ces deux applications sont donc qualifiées de « flop »[37].

Démontrer la nécessité de cet outil suppose également, pour l'APD, qu'il constitue « la mesure la moins intrusive »[38] dans les libertés citoyennes. Or, en Belgique notamment, l'envie du gouvernement de disposer d'un outil numérique semble éclipser cet aspect. Pourtant, les masques, la distance physique, les tests, les quarantaines sont des éléments qui, à la différence des applications de traçage, fonctionnent à coup sûr dans la lutte contre une pandémie, ne supposent pas de dépenser des sommes importantes en consultants et, ne créent pas de risques liberticides à long terme. Le manque d'attention à cet égard est d'autant plus regrettable qu'une application ne peut pas fonctionner seule. Il faut notamment un système de tests très bien rôdé et des moyens humains importants pour accompagner l'utilisation du traçage numérique[39].

Quant à la *proportionnalité au sens strict,* l'APD insiste sur l'importance de démontrer qu'« il existe un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées ». En d'autres termes, « les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées »[40]. Ces éléments n'étant pas démontrés, l'APD ne valide pas l'application belge.

La mise en balance des avantages et des inconvénients d'une application de traçage suppose que l'on approfondisse les risques que génère pareil outil, ce que l'on fait dans les lignes qui suivent.

35. https://fr.statista.com/infographie/23207/part-de-la-population-telechargements-applications-tracage-covid-19-stopcovid/
36. https://www.rtbf.be/info/societe/detail_coronavirus-l-application-coronalert-telechargee-par-un-million-de-belges?id=10607469.
37. Entre autres nombreuses communications à ce sujet, v. not. https://www.lopinion.fr/edition/politique/coronavirus-l-application-stopcovid-fait-flop-222215 ; https://plus.lesoir.be/341784/article/2020-12-04/coronalert-le-flop
38. APD, avis n° 34/2020, n° 7.
39. Par exemple, à Singapour et en Corée du Nord, des moyens humains importants ont été déployés pour accompagner les personnes ayant reçu une alerte sur leur téléphone et les amener à respecter le confinement. À ce sujet, v. Observatoire international sur les impacts sociétaux de l'IA et du numérique (Canada), *Efficacité et enjeux sociétaux des apps de traçage de contacts,* préc., https://observatoire-ia.ulaval.ca/3674/
40. APD, avis n° 34/2020, n° 8.

III. LES RISQUES GÉNÉRÉS PAR LE TRAÇAGE NUMÉRIQUE

A. – Des risques techniques et démocratiques

Les risques émanant des applications de traçage peuvent être qualifiés de techniques et de démocratiques.

Parmi les risques techniques, la technologie « Bluetooth », à laquelle recourent « Stopcovid » en France, et « Coronalert » en Belgique, notamment, fait beaucoup parler d'elle. En effet, cette technologie n'a pas été conçue pour le traçage numérique et provoque plusieurs difficultés. Parmi celles-ci, le fait que cette technologie est « aveugle » pourrait amener à signaler à une personne qu'elle est possiblement contaminée alors qu'elle se trouvait derrière une paroi de plexiglas ou que chacun portait un masque au moment où l'application a identifié une possible contamination. Ce « faux positif » risque de créer un stress inutile, et d'inciter la personne à aller se faire tester, encombrant inutilement les centres de test et ralentissant le « testing » encore davantage. C'est d'ailleurs pour éviter les « faux négatifs » et les quarantaines inutiles que des entreprises demandent à leurs employés de ne pas télécharger l'application de traçage[41].

Au-delà des problèmes techniques, les applications de traçage soulèvent des risques démocratiques, au sens où ils modifient ou pourraient modifier l'attitude et le rôle du citoyen dans la cité.

B. – La paradoxale liberté sous surveillance

Le traçage numérique renforce-t-il la tolérance de la population à la surveillance de l'État ? C'est à craindre. À cet égard, les travaux de Michel Foucault sont éclairants. Ils soulignent le lien étroit entre chaque épidémie et la mise en place d'une nouvelle stratégie d'organisation de la société, celle-ci s'affinant et évoluant vers une surveillance plus étroite de la population par le pouvoir en place[42].

Ainsi, vers les XIII[e] et XIV[e] siècles, lors de l'épidémie de lèpre, le pouvoir organise l'exclusion des malades. Les lépreux sont envoyés dans des territoires indéfinis ou enfermés dans des léproseries. L'idée est d'organiser une césure spatiale entre les lépreux et la communauté.

Face à la peste, au XVIII[e] siècle, la stratégie est tout autre. L'inclusion se substitue à l'exclusion, en multipliant les quarantaines et en affinant le contrôle

41. L'article évoque l'entreprise GSK au Royaume-Uni et en Belgique https://www.rtbf.be/info/societe/detail_l-application-coronalert-une-amie-genante-pour-les-entreprises?id=10604686.
42. A ce sujet, v. not. M. Foucault, *Les anormaux. Cours au Collège de France 1974-1975*, Paris, Gallimard/Le Seuil, 1999.

de l'espace et de la population, qui s'exerce en continu. Le pouvoir n'exclut plus, il observe. Chaque quartier, chaque rue, est placé sous le contrôle d'inspecteurs. Le gouvernement, qui voit ses pouvoirs étendus, utilise des instruments d'analyse et de collecte de données. La politique de surveillance est née. Ainsi, « alors que la lèpre appelle la distance, la peste implique une approche de plus en plus fine de la société, jusqu'à la connaissance du moindre individu, en fonction de la norme de santé »[43].

Dans quel but, se demande Foucault ? Celui de la normalisation des individus. C'est l'idée que chaque personne surveillée, pensant être regardée, intègre la norme de bonne conduite[44]. Au risque que s'éteignent la spontanéité des attitudes, l'originalité des comportements, et donc, la liberté individuelle. Pour Foucault, ce processus de normalisation est au service du « contrôle des populations, non plus régi sur le mode du châtiment, mais de la discipline, visant (...) à contrôler des masses de population »[45], et il sous-tend un « ordre juridique totalitaire, qui enferme l'autonomie individuelle par une réglementation tentaculaire, laquelle codifie intégralement cette fois-ci ce qu'il faut faire », « s'infiltrant dans tous les recoins de la vie de chaque individu tout en gérant des populations entières »[46].

Dès lors que la technologie est utilisée pour lutter contre le coronavirus, on peut y voir un renforcement de cette organisation disciplinaire émanant du pouvoir en place. C'est encore plus vrai aujourd'hui, puisque l'État possède une masse de données numériques sur chaque aspect de nos vies ainsi que des outils puissants permettant de regrouper ces données, les comparer, et identifier des « profils suspects ». Avec le traçage numérique, le public, percevant la technologie comme une solution pour sortir de la crise sanitaire et économique, risque d'intérioriser la nécessité d'utiliser ces outils pour réguler la société, de la banaliser et d'accepter, progressivement, une surveillance technologique généralisée de la population.

Pourtant, la technologie pourrait être utilisée pour responsabiliser les individus, et non les surveiller. Pourquoi ne pas songer d'abord à des outils qui aideraient les citoyens à respecter les gestes barrière, en calculant la distance sociale, par exemple ? Ou un « bulletin météo » en ligne indiquant les régions dans lesquelles le virus augmente, de manière à inciter ces habitants-là à être particulièrement prudents, voire à se confiner le temps que les chiffres descendent ?

Pourtant, dans le chef des gouvernements actuels, c'est le choix de surveiller la population, et non de la responsabiliser, qui prime. Dans ce contexte de

43. M. Pingeot, « Le confinement et Foucault », oct. 2020, Festival Philosophia, http://www.festival-philosophia.com/une-notion-un-auteur/le-confinement-et-foulcaut/
44. M. Foucault, *op. cit.*, p. 46.
45. O. Whright, « Norme, normalité et normalisation chez Michel Foucault », 6 janv. 2014, https://www.o-wright.com/uploads/2/6/4/3/26432010/dissertation_-_olivier_wright_-_norme_normalite_et_normalisation_chez_michel_foucault.pdf
46. *Id.*

méfiance, il est donc particulièrement important que les outils technologiques utilisés par l'État soient balisés par le Parlement, dans leur forme, mais aussi dans leur durée, qui doit être la plus éphémère possible. Or des expériences passées montrent que les atteintes aux libertés, annoncées comme provisoires, le temps de traverser une crise, ont tendance à devenir permanentes... Le Plan Vigipirate est un bon exemple de mesure provisoire de surveillance devenue permanente[47]. Ainsi, s'agissant de la pandémie actuelle, on peut légitimement douter que les États décréteront un jour « la fin de la guerre contre le coronavirus » comme on signerait l'armistice...

C. – La place donnée à la « loi des algorithmes »[48]

En incitant les individus à télécharger une application de traçage pour sortir de la crise, on les encourage à faire confiance à des outils qu'ils ne comprennent pas et à propos desquels ils reçoivent peu, voire pas, d'explication.

En Belgique, et au-delà de la crise du Covid, il est frappant de constater que, dès les premières initiatives concernant l'e-gouvernement, la priorité a été donnée à la mise en place de technologies pour renforcer l'efficacité administrative. Très peu d'outils sont mis à disposition du public pour visualiser, comprendre, et dès lors contrôler ce qu'il advient, par exemple, des données qu'il est contraint de confier à l'État. Dans ce contexte, il n'est pas exagéré de dire que l'État avance en limousine tandis que le citoyen avance à pied[49].

En particulier, les algorithmes utilisés par l'État doivent retenir notre attention. En effet, bien qu'un algorithme, de par son mystère et sa complexité, renvoie une apparence de neutralité et d'objectivité scientifique, il n'en n'est rien. Un algorithme est, certes, une suite d'instructions techniques. Mais ce n'est pas une chose pure et vierge qui descendrait du ciel pour nous donner la vérité et nous montrer le sens de la Justice. Cette suite d'instructions techniques est décidée par un être humain, appelé « développeur » ou « programmateur ». Lorsqu'il crée un algorithme, cette personne, consciemment ou non, pose des choix qui reflètent ses propres valeurs, sa propre sensibilité en décidant des données à utiliser en

47. À ce sujet, v. not. *Le Monde*, 24 avr. 2015, « Plan Vigipirate : comment un dispositif exceptionnel est devenu permanent », accessible ici https://www.lemonde.fr/les-decodeurs/article/2015/04/24/plan-vigipirate-comment-un-dispositif-exceptionnel-est-devenu-permanent_4621647_4355770.html
48. Selon l'expression de B. Barraud, « Le coup de data permanent : la loi des algorithmes », *RDLF* 2017, accessible ici http://www.revuedlf.com/droit-fondamentaux/le-coup-de-data-permanent-la-loi-des-algorithmes
49. Selon D. W. Schartum, « within a democracy, citizen should not be left as pedestrians when the authorities drive limousines ». V. D. W. Schartum, « Access to Government-Held Information : Challenges and Possibilities », *The Journal of Information Law and Technology* 1998/1, § 7.1.

priorité, des critères à appliquer et du poids à leur donner, etc.[50] Or, une fois l'algorithme utilisé à l'échelle de la société, il a un impact sur l'ensemble de la population. Le choix algorithmique est donc un choix de société.

Depuis plusieurs années, les algorithmes sont utilisés pour renforcer l'efficacité de l'État, quel que soit le secteur concerné : secteur de la santé mais aussi lutte contre la fraude sociale, contre la fraude fiscale, etc. En Belgique, un récent arrêté ministériel organise d'ailleurs l'application d'algorithmes aux données Covid récoltées dans le cadre du traçage, dans le but de contrôler les quarantaines des travailleurs, voire plus[51].

Compte tenu de l'impact des algorithmes utilisés par l'État sur l'ensemble des citoyens, changer le paramètre d'un algorithme aura le même effet qu'une réforme législative. Il ne faudrait pourtant pas que la « loi des algorithmes », secrète, opaque, incompréhensible, se substitue à « la loi du Parlement », publique, transparente et, en principe, compréhensible. En d'autres termes, le choix algorithmique étant *de facto* un choix de société, il devrait être débattu par le Parlement et encadré clairement par celui-ci. Il y aurait lieu d'organiser, par exemple, la transparence de ces algorithmes en faisant la lumière sur leurs concepteurs, les objectifs poursuivis, les données utilisées. Il y aurait lieu aussi d'en instituer le contrôle pour s'assurer, notamment, de l'absence de « biais » qui pourraient créer de graves discriminations[52]. Autant d'aspects importants qui, actuellement, sont passés sous silence et risquent de conduire nos sociétés vers une automatisation grandissante. Celle-ci serait inquiétante, car ces puissants outils pourraient échapper à la compréhension des gouvernements qui les mettent en place. De plus, en automatisant la société, ils pourraient conduire à la couper du lien avec le citoyen, pourtant essentiel à la démocratie. Un citoyen qui, ne comprenant plus le fonctionnement de l'État, capitulerait, conduisant la société à sa perte. Car sans remise en question, sans débat démocratique, en ne s'alimentant plus de rien, la société est destinée à tourner sur elle-même, à s'asphyxier et finalement à mourir…

*
* *

La question du traçage numérique charrie les lames de fond de nos sociétés démocratiques. Peut-on prendre prétexte de l'urgence et de la technicité du sujet

50. À ce sujet, v. C. O'Neill, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, USA, Crown Books, 2016.
51. V. E. Degrave, « Les citoyens contrôlés via leurs données covid ? Le "datamatching" et le "datamining" utilisés par l'État », *Journal des Tribunaux* 2021, p. 125-128.
52. Les « biais algorithmiques » sont liés au fait qu'un algorithme résulte du choix fait par l'humain qui l'a conçu et qui y met – consciemment ou non – sa propre sensibilité. Ces biais peuvent entraîner des conséquences racistes, sexistes, qui nuisent aux pauvres, etc. Utilisés à l'échelle d'une population, de tels biais peuvent conduire à « automatiser les inégalités » selon l'expression de V. Eubanks (*Automating inequality. How high-tech tools profile, police and punish the poor*, New York, St Martin's Press, 2018).

pour confier les clés de l'État à des « experts », des techniciens dont nous ne connaissons ni les intérêts politiques, ni économiques ?

En acceptant la mise en place de cet outil dont la nécessité n'est pas démontrée et les risques techniques pourtant bien réels, mène-t-on les citoyens vers la banalisation d'une surveillance technologique généralisée, soumise à la loi des algorithmes plutôt qu'à la loi du Parlement ? Laisse-t-on ainsi le gouvernement mettre en place des outils très puissants dont il n'a peut-être déjà plus la maîtrise ?

Face à tant de questions non résolues, comment garder confiance dans un État technologiquement de plus en plus puissant, mais aussi de plus en plus opaque ?

Le traçage numérique interroge cette confiance, essentielle au bon fonctionnement de la démocratie. D'ordinaire, l'État ne demande pas au citoyen s'il accepte de lui confier ses données. Mais, de manière peu habituelle, le traçage numérique requiert la bonne volonté du citoyen pour atteindre le succès. Bien que la réalité de cette volonté libre soit discutable, les premiers retours d'expérience montrent un lien entre la confiance en l'État et le succès du téléchargement des applications de traçage. Sans confiance, pas de téléchargements suffisants. On doit y voir le constat rassurant d'une population qui n'est pas encore anesthésiée et reste attentive à la balance entre l'efficacité et la protection des libertés, même lorsque la santé est en jeu.

Quoi qu'il en soit, le choix de faire confiance à la technologie pour sortir d'une pandémie ne peut être laissé à chaque individu, abandonné seul devant son téléphone. C'est, collectivement, forts de la conscience de nos libertés, que nous devons, aujourd'hui, poser ce choix technologique déterminant.