STOPCOVID

AVIS DU CONSEIL NATIONAL DU NUMÉRIQUE

conseil national
du numérique

Contexte de saisine

Dans le cadre de la réponse à la crise du COVID-19, **le secrétaire d'État chargé du Numérique a saisi[1] le Conseil national du numérique pour émettre un avis sur les modalités de fonctionnement et de déploiement de l'application pour téléphones mobiles StopCOVID**, dont le développement a été annoncé le 8 avril 2020[2].

Le Conseil national du numérique a veillé à être le plus représentatif possible dans ses auditions[3]. Fidèle à sa mission d'éclaireur des transformations numériques, il a souhaité mettre en exergue les questions qu'il est indispensable de se poser en préalable au développement d'une application de gestion d'épidémie à destination de l'ensemble des citoyennes et des citoyens. Ces questions concernent tant l'application elle-même que la façon dont elle sera déployée et les tensions entre différentes libertés fondamentales dont elle peut être la source.

Le Conseil est conscient de ne fournir qu'une lecture sous forme de « photographie », représentative de nos connaissances à la date de sa publication et qui pourra par conséquent être vite rendue obsolète. Le développement de l'application et de toutes les briques qui la composent n'est pas terminé, ce qui rend difficile le fait de se prononcer définitivement. **Pour établir son avis, le Conseil s'est donc appuyé sur les éléments déjà rendus publics : les déclarations successives du secrétaire d'État chargé du Numérique, ainsi que la publication du protocole ROBERT sur lequel sera basée l'application StopCOVID**[4].

Avis du Conseil national du numérique

Le Conseil est favorable au principe de StopCOVID, en tant que brique d'une stratégie plus globale

Le Conseil national du numérique **estime que les applications d'historique de proximité peuvent être utiles pour lutter contre le COVID-19, et doivent pour cela s'inscrire dans une stratégie plus globale de santé publique**. Ces applications doivent être utilisées pour informer, aider et responsabiliser, plutôt que pour contrôler, stigmatiser ou réprimer les individus. **Les citoyennes et citoyens doivent être rendus acteurs de la protection de leur santé et de celle des autres dans un objectif d'intérêt public.**

Le Conseil tient cependant à souligner que **ce type d'application, comme StopCOVID, ne sont qu'une partie de la réponse sanitaire** dont l'efficacité dépendra sûrement plus des mesures de distanciation sociale et de

[1] *Cf.* lettre de saisine en annexe.
[2] UNTERSINGER Martin, HECKETSWEILER Chloé, BEGUIN François et FAYE Olivier, «L'application StopCovid retracera l'historique des relations sociales : les pistes du gouvernement pour le traçage numérique des malades», *LeMonde.fr*, 8 avril 2020.
[3] *Cf.* personnes auditionnées en annexe.
[4] INRIA, *Publication du protocole ROBERT (ROBust and privacy-presERving proximity Tracing)*, 18 avril 2020.

la mise à disposition de tests. Ainsi le Conseil suggère de renommer l'application "AlerteCOVID" qui est plus en adéquation avec l'objectif visé (recommandation n°8).

Le respect de la souveraineté numérique est une condition fondamentale afin de garantir la confiance dans StopCOVID. **Le Conseil recommande donc qu'une seule application spécifiée par l'État soit mise en œuvre et libre de tout soupçon d'intérêt économique sous-jacent** (recommandation n°3)**.**

Le Conseil national du numérique considère, **sous réserve de la prise en considération des remarques ci-dessous, en particulier sur le respect des droits et libertés fondamentaux, ainsi que des recommandations détaillées à la suite du présent avis, que le développement de l'application StopCOVID est une piste que le gouvernement se doit d'envisager**, dans une stratégie globale de lutte contre la pandémie.

Le Conseil pose les conditions nécessaires pour garantir l'intérêt général et l'État de droit

Le Conseil rappelle qu'une relation de confiance robuste constitue la première des conditions à l'implication des citoyennes et des citoyens. Cette relation doit se fonder sur une transparence totale et des moyens de contrôle et de suivi indépendants.

À ce titre, le Conseil estime utile de **créer un comité de contrôle, avec des parlementaires, des chercheurs et des citoyens-experts, disposant d'un pouvoir d'arrêt de l'application** (recommandation n°1). Ce comité de contrôle pourrait s'assurer de la bonne mise en œuvre du système et garantir le respect des valeurs qui le fondent tout au long de son usage. Le Conseil souhaite aussi insister sur **l'importance de la limitation dans le temps** (recommandation n°2) du système, qui doit rester une réponse exceptionnelle à une crise qui l'est aussi.

Ce dispositif, tout en tenant compte des risques existants pour les libertés et droits fondamentaux, doit s'insérer dans une stratégie exceptionnelle de santé plus globale qui relève de l'ordre public sanitaire et donc de l'intérêt général.

Le Conseil insiste sur les facteurs-clefs de réussite pour une appropriation citoyenne : inclusion numérique, accessibilité et loyauté de l'information

Le Conseil tient par ailleurs à insister sur le fait que **le succès de l'usage** de l'application, dans le cas où le gouvernement retiendrait ce choix, **dépendra grandement des efforts de communication et de transparence** que ce dernier fournira (recommandations n°5 à 9), **ainsi que des dispositifs destinés à inclure dans cette stratégie les personnes exclues du numérique**.

Les personnes exclues ou éloignées du numérique ne forment pas un ensemble homogène. Les difficultés à accéder ou à utiliser l'application peuvent être matérielles, cognitives, physiques, et **les réponses à apporter**

dépendent fortement du public qui les reçoit, qu'il soit en capacité de se former ou qu'il ait besoin d'un accompagnement direct ou d'une intermédiation.

Afin d'apporter des réponses rapides, il faut **mobiliser au plus vite les acteurs de terrain** (travailleurs sociaux, structures de médiation, associations, collectivités, etc.) **pour bénéficier de leur maillage du territoire, de leur connaissance fine des publics fragiles et de leur capacité à organiser l'accompagnement** (recommandation n°10). De l'évaluation des manques et des besoins à l'accompagnement lors du déploiement de l'application, ils doivent être entendus, outillés et soutenus par le gouvernement.

À cet égard, une attention particulière est à porter à la diversité des **outillages et à la formation, en urgence, des aidants, travailleurs sociaux, médiateurs et accompagnateurs** qui auront à traiter de ces questions (recommandation n°11). Il conviendra de leur apporter des éléments qui leur permettront d'accompagner l'usage de l'application et de lutter contre les idées reçues qui entoureront celle-ci.

Pour répondre aux problématiques d'accessibilité et d'ergonomie de l'application sur les téléphones et les autres supports potentiels sur lesquels elle sera déployée, préalables à son adoption par le plus grand nombre, **une attention particulière doit être accordée à l'expérience utilisateur** (recommandations n°12 à 15), à l'interface de l'outil et à sa phase de test.

Recommandations

Confiance et gouvernance

Recommandation n°1 : Créer un comité de contrôle, avec des parlementaires, des chercheurs et des citoyens-experts, disposant d'un pouvoir d'arrêt de l'application.
Recommandation n°2 : Encadrer l'application par un décret fixant les conditions de sa mise en œuvre, sa durée dans le temps et des garanties sur la protection des données (base légale, finalité, proportionnalité, durée de conservation des données et du système, minimisation des données, responsable de traitement, voies de recours...).

Souveraineté

Recommandation n°3 : Favoriser une seule application pour la France, sous l'autorité du Ministère de la Santé.
Recommandation n°4 : Élargir les prérogatives des autorités de contrôle pour diminuer la dépendance aux fabricants de systèmes d'exploitation mobiles.

Transparence

Recommandation n°5 : Publier le code source de l'application et des systèmes associés ainsi que leur documentation sous des licences libres et des éléments de vulgarisation.
Recommandation n°6 : Expliciter le processus déterminant lorsqu'un contact est à risque.

Communication

Recommandation n°7 : Permettre le signalement des mésusages et des dérives de l'application en créant un numéro vert dédié (pression de l'employeur à installer, interdiction d'accès dans un lieu public).
Recommandation n°8 : Renommer l'application « AlerteCOVID » pour ne pas lui faire porter de fausses promesses.
Recommandation n°9 : Organiser des séances de questions-réponses entre les citoyens et les responsables politiques, par exemple à travers des directs sur des médias généralistes (sur les mêmes modalités, organiser des séances à destination de la communauté technique et de la médiation).

Fracture numérique

Recommandation n°10 : Mobiliser les acteurs de terrain (collectivités, structures de médiations, associations) pour évaluer les besoins et accompagner les plus éloignés du numérique, voire participer à leur équipement.

Recommandation n°11 : Assurer la formation des aidants et des médiateurs en mobilisant des solutions existantes.

Expérience utilisateur

Recommandation n°12 : Simplifier au maximum l'installation et l'utilisation de l'application en épurant son design et en utilisant le français facile à lire et à comprendre (FALC).
Recommandation n°13 : Clarifier les procédures à suivre en cas de test positif et de réception d'une notification.
Recommandation n°14 : Proposer une version simplifiée des conditions générales d'utilisation.
Recommandation n°15 : Créer de l'engagement en rendant le citoyen actif dans la santé de tous, en affichant les statistiques et les consignes sanitaires.

Analyse détaillée

Quels sont les objectifs de l'application StopCOVID ?

Dans son avis du 23 mars 2020, le Conseil scientifique COVID-19 note que « *le confinement est actuellement la seule stratégie réellement opérationnelle, l'alternative d'une politique de dépistage à grande échelle et d'isolement des personnes détectées n'étant pas pour l'instant réalisable à l'échelle nationale* »[5]. La stratégie sanitaire de dépistage et d'isolement consiste à mener des enquêtes auprès des personnes infectées pour identifier et tester les autres personnes avec qui elles ont eu des contacts à risque[6]. Ces autres personnes pouvant être devenues porteuses du virus, **la rapidité des enquêtes est un élément déterminant pour limiter la propagation du virus**.

Dans son avis du 2 avril 2020, le Conseil scientifique COVID-19 propose ainsi plusieurs critères de sortie de confinement, dont l'un est de pouvoir « *s'assurer que les éléments d'une stratégie post-confinement seront opérationnels, incluant notamment […] de nouveaux outils numériques permettant de renforcer l'efficacité du contrôle sanitaire de l'épidémie* »[7]. Ainsi, l'application **StopCOVID est développée pour pouvoir être rapidement mise en place si elle était jugée utile dans une stratégie post-confinement**.

À l'étranger, des applications d'historique de proximité ont été développées dans le but d'automatiser et d'accélérer une partie de ces enquêtes, en complément des dispositifs humains. TraceTogether[8], développée par le gouvernement singapourien, est probablement la plus connue de ces applications[9], même si de nombreuses initiatives publiques, privées ou de la société civile sont en train d'émerger en France et ailleurs dans le monde. En Corée du Sud, l'épidémie a été contenue, entre autres, grâce à une politique d'enquêtes très poussées menées par de nombreux fonctionnaires qui ont retracé l'historique des rencontres des porteurs de virus et permis d'identifier et d'isoler les personnes qu'ils auraient pu contaminer[10].

De manière générale, les membres du Conseil national du numérique estiment que le numérique peut être utile pour lutter contre le COVID-19 et qu'il doit être utilisé pour informer, aider et responsabiliser, plutôt que pour contrôler, stigmatiser ou réprimer les individus. Les citoyennes et citoyens doivent être rendus acteurs de la protection de leur santé et de celle des autres dans un objectif d'intérêt général.

---

[5] CONSEIL SCIENTIFIQUE COVID-19, Avis du Conseil scientifique du 23 mars 2020, 23 mars 2020.

[6] Ces enquêtes font partie des missions de veille sanitaire et sont déjà obligatoires pour certaines maladies, comme la rougeole. Voir KORDA Robin, «Coronavirus : comment des «enquêteurs» remontent le fil des contaminations», *Le Parisien*, 28 février 2020.

[7] CONSEIL SCIENTIFIQUE COVID-19, *Avis du Conseil scientifique - État des lieux du confinement et critères de sortie*, 2 avril 2020.

[8] Voir le site de l'application Trace Together.

[9] Des applications similaires ont été développées : Flux Phone est une application mobile développée par des chercheurs de Cambridge qui suit le comportement des gens pendant une épidémie et qui pourrait être utilisée pour limiter la propagation du COVID-19.

[10] MESMER Philippe, «En Corée du Sud, le respect de la vie privée au défi du traçage des contaminés au Covid-19», *Le Monde Pixel*, 5 avril 2020.

Comment fonctionne StopCOVID ?

Les applications d'historique de proximité ont toutes le même objectif : enregistrer une liste des autres utilisateurs de l'application, avec qui l'utilisateur est entré en contact, et les prévenir *a posteriori* si celui-ci se révélait infecté par le COVID-19.

Pour enregistrer la liste des personnes rencontrées, StopCOVID s'appuie sur la technologie *Bluetooth Low Energy (BLE)*[11], technologie de communication sans-fil dont la portée est de quelques mètres : si un téléphone détecte un autre utilisateur de l'application, il est probable que celui-ci se trouve à proximité du téléphone. Chaque rencontre avec un autre utilisateur de l'application est enregistrée, créant ainsi un « historique de proximité ».

Lorsqu'un utilisateur est testé positif au COVID-19 et avec l'accord de celui-ci, l'application transmet l'historique de proximité à un serveur central, opéré par les autorités sanitaires. En fonction des caractéristiques de chaque rencontre dans cette liste (durée et distance), les utilisateurs les plus à risque sont alertés via une notification sur leur application.

Même si toutes les applications d'historique de proximité partagent le même objectif, les choix techniques ont des répercussions importantes sur le niveau de partage des données de l'utilisateur, pouvant entrer en concurrence avec l'efficacité de la prévention. Par exemple, le fait que *TraceTogether* ne soit pas anonyme permet de mieux articuler les enquêtes sanitaires manuelles et l'application.

Quels leviers activer pour renforcer la confiance dans l'application ?

Quelles sont les garanties annoncées en matière de vie privée et de protection des données ?

La surveillance à grande échelle des contacts entre les personnes présente des risques d'atteinte à des libertés et droits fondamentaux, comme cela a été souligné par les associations de protection des droits et libertés numériques[12], mais peut être justifiée par la protection de la santé. Les membres du Conseil

[11] La technologie BLE n'a cependant pas été développée pour mesurer des distances entre les appareils et sa précision pour cette tâche est donc limitée.

[12] En ce sens, l'Observatoire des libertés et du numérique (OLN) estime que « *les utilisations envisagées de nos données personnelles (applications utilisant le Bluetooth pour le suivi des contacts) ou déjà mises en œuvre (géolocalisation) constituent une grave atteinte à nos libertés et ne sauraient être autorisées, ni utilisées sans notre consentement.* » *In* : Communiqué de l'OLN, Paris, le 8 avril 2020, *La crise sanitaire ne justifie pas d'imposer les technologies de surveillance*. *Adde* : La Quadrature du Net estime que « *l'utilisation d'une application dont les objectifs, les techniques et les conditions mêmes d'usage portent des risques conséquents pour notre société et nos libertés (i.e sur les discriminations, la surveillance et l'acclimatation sécuritaire), pour des résultats probablement médiocres (voire contre-productifs), ne saurait être considérée comme acceptable pour nous – tout comme pour beaucoup de Français·es*. ». *In* : La Quadrature du Net, *Nos arguments pour rejeter StopCovid*, 14 avril 2020.

.

national du numérique ne sauraient nier l'absence de risques sur les droits et libertés fondamentaux des citoyennes et citoyens liés à l'usage de l'application StopCOVID[13]. Ils considèrent que ces risques sont limités, d'une part, car les citoyennes et citoyens pourront choisir d'utiliser ou non cette application et, d'autre part, car des garde-fous juridiques existent en cas d'abus[14]. Par ailleurs, **ce dispositif, tout en tenant compte des risques existants pour les libertés et droits fondamentaux, doit s'insérer dans une stratégie exceptionnelle de santé plus globale qui relève de l'ordre public sanitaire et donc de l'intérêt général.**

Parmi les éléments mis à la connaissance du CNNum, ceux concernant les impacts de cette application sur la vie privée[15] peuvent pour l'instant se résumer ainsi :

- l'application est fondée sur des identifiants pseudonymisés et temporaires.
- L'identité réelle (nom, prénom) ou le numéro de téléphone d'un utilisateur n'est jamais connu de l'application, du serveur central opéré par l'autorité sanitaire ni même d'autres utilisateurs.
- Il ne sera pas possible, si l'on reçoit une notification, d'obtenir des informations concernant le contact qui a été déclaré malade ni de savoir quand il a été croisé.
- Les données collectées seront uniquement utilisées dans le cadre de l'application StopCOVID et ne sont conservées que le temps nécessaire pour le bon fonctionnement de l'application.
- Les utilisateurs de l'application ne peuvent pas se réidentifier entre eux, même en recoupant avec d'autres informations.
- L'application a été conçue, en respectant le principe de protection de la vie privée et de protection des données (approche dite *privacy by design*) avec un principe de minimisation des données collectées.
- La technologie *Bluetooth* est considérée comme étant moins intrusive quant aux données personnelles et à la vie privée des citoyens que la géolocalisation.

Le respect du règlement 2016/679/EC sur la protection des données personnelles (règlement RGPD) et de la directive 2002/58/EC (directive dite "ePrivacy ") sont indispensables pour instaurer la confiance et créer les conditions de l'acceptabilité sociale de toute solution. Il convient de s'assurer que l'application StopCOVID respecte les grands principes de la protection des données personnelles : identifiants chiffrés et pseudonymisés, non-identification, respect du principe de limitation des finalités, minimisation des données, nécessité, proportionnalité, sécurité, durée limitée de conservation/suppression, contrôle, existence de voies de recours, transparence et droit d'accès, garanties sur le caractère temporaire et le démantèlement du système quand la situation ne l'exige plus… **Le Conseil estime que le responsable de**

[13] V. notamment : Interview de CHRISTAKIS Théodore, «En temps de crise, il y a toujours un risque important d'adopter des mesures liberticides», *NextINPACT*, 07 avril 2020.
[14] V. notamment : BLANDIN Annie (entretien recueilli par Philippe GUEGAN), «Coronavirus. L'application « Stop Covid », outil de surveillance ou instrument d'entraide ?», Ouest France, 20 avril 2019.
[15] Le modèle de sécurité et des attaques pouvant remettre en cause certaines de ces affirmations sont présentées dans l'avis détaillé. Voir aussi le travail de chercheurs spécialistes en matière de cryptographie, sécurité ou droit des technologies selon lequel le traçage automatisé des contacts à l'aide d'une application sur smartphone comporte de nombreux risques, indépendamment des détails de fonctionnement de cette application : BONNETAIN, CANTAEAUT, CORTIER et alii, «Le traçage anonyme, dangereux oxymore - Analyse de risques à destination des non-spécialiste», version du 21 avril 2020.

traitement devrait être clarifié. Privilégier les autorités de santé comme responsables de traitement pourrait permettre de renforcer la confiance des citoyens[16].

<table>
<tr><th colspan="2">CONTROVERSE</th></tr>
<tr><td colspan="2">L'application StopCOVID revêt-elle un caractère sanitaire ?</td></tr>
<tr><td>Une application s'insérant
dans un ordre public sanitaire</td><td>Un simple outil numérique d'aide
pour faciliter le travail des épidémiologistes</td></tr>
<tr><td>L'application StopCOVID s'intègre dans des débats sur le « lien entre ordre public et droits fondamentaux et (...) sur les rapports entre liberté et sécurité sanitaire »[17]. L'application s'insère en effet dans un ensemble de politiques publiques pour lutter contre la pandémie qui relève donc d'un ordre public sanitaire marqué par « la recherche de sécurité pour la santé »[18]. Les données des citoyennes et citoyens qui utiliseraient l'application, si celle-ci s'avère efficace, ont par nature vocation à contribuer à l'intérêt général, car l'utilisation individuelle de l'application pourrait participer plus largement à la protection collective de la santé publique. Dès lors, on peut s'interroger sur les données concernées, et leur nature, qui dépendent également de la finalité de l'application StopCOVID : s'agit-il d'un dispositif médical ou</td><td>L'application devrait uniquement viser à informer les individus du fait qu'ils ont été en contact étroit avec quelqu'un qui est porteur du virus confirmé, afin d'interrompre les chaînes de contamination le plus tôt possible. Dès lors, cette application a vocation à faciliter le travail, actuellement réalisé à la main, des enquêtes épidémiologiques pour identifier d'éventuels porteurs du virus. L'application ne serait donc pas un outil sanitaire, mais seulement un outil numérique d'optimisation du suivi des contacts. Seule une intervention humaine peut qualifier les contacts à risque et traiter ainsi les cas de faux positifs et de faux négatifs. Lors de son audition, le président du Conseil scientifique COVID-19 recommandait donc, en complément des outils numériques, de mettre en place une brigade de traçage pour repérer les « cas-contacts » des personnes infectées par le Covid-19[19]. Par ailleurs, certains considèrent que</td></tr>
</table>

[16] Dans ses lignes directrices du 21 avril 2020 sur le contact tracing (point 25), le Comité européen de la protection des données considère que les autorités nationales de santé pourraient être les responsables de traitement, mais que d'autres responsables de traitement peuvent également être envisagés. EUROPEAN DATA PROTECTION BOARD, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020.

[17] HOURDEAUX Jérôme, «RENARD Stéphanie, « Cette crise menace l'égalité et interroge sur la solidarité »», Entretien *Médiapart*, 15 avril 2020.

[18] *Ibid.*

[19] Mercredi 15 avril 2020, le président du Conseil scientifique du COVID-19, Jean-François Delfraissy déclarait devant les membres de la mission de contrôle du Sénat sur la crise sanitaire que « *les Coréens ont une brigade (...) pour traquer les contacts. (...) Il y a de l'humain derrière le numérique. (...) Mais ça, on ne l'a pas en France! Si on ne l'a pas, une application numérique ne marchera pas*.» *In* : PUBLIC SÉNAT, «Traçage numérique pendant l'épidémie: audition de Jean-François Delfraissy, président du conseil scientifique COVID-19», 15 avril 2020.

d'une application de confort ? Sont-elles des données de santé ? Quelles définitions des données *Bluetooth* dans ce contexte ?	l'architecture du système fait qu'il ne traite les données de santé que sur l'appareil de l'utilisateur.

Encadrer l'application par un décret

Le Gouvernement a fait le choix de privilégier le volontariat. Cela signifie que chaque individu est libre de télécharger ou non l'application ou encore de mettre fin à son utilisation, avec la garantie que les données sur son téléphone et sur le serveur soient effacées définitivement, avec un arrêt du service et des collectes une fois la période de crise achevée (et ce, même si l'application reste installée). **L'application pourrait reposer sur la base légale du consentement ou sur celle de l'intérêt public[20] . Le Conseil a toujours soutenu le principe selon lequel les personnes doivent pouvoir maîtriser pleinement leurs données personnelles à tout moment. Plusieurs institutions considèrent que le volontariat permet de renforcer la confiance des citoyens**[21].

Afin de renforcer la transparence et d'offrir un cadre juridique précis, clair et offrant toutes les garanties, **le Conseil considère que l'application devrait être encadrée par un décret fixant les conditions de son application et les garanties qui l'entourent**, notamment pour :

- **Préciser la base légale,**
- **Définir avec précision les finalités de l'application** qui doivent être limitées à la gestion de la crise sanitaire et exclure toutes les finalités qui ne sont pas liées à la lutte contre le COVID-19[22],
- **Prévoir le caractère volontaire de l'application** et le fait qu'il n'y ait pas de discriminations ou de conséquences négatives en cas de refus de télécharger l'application,
- Clarifier les règles applicables pour les mineurs ou majeurs protégés,
- **Définir avec précision le responsable de traitement** et ses obligations,
- **Fixer toutes les garanties en matière de protection des données et de la vie privée**, y compris les voies de recours,
- **Définir les modalités de contrôle**.

[20] Dans son ses lignées directives précitées du 21 avril (point 29), le Comité européen de la protection des données note que le simple fait que l'utilisation d'applications de *contact tracing* ait lieu sur une base volontaire ne signifie pas que le traitement des données personnelles doive nécessairement avoir pour base légale le consentement. Lorsque les pouvoirs publics fournissent un service basé sur un mandat assignées par et conformément aux exigences fixées par une loi, il apparaît que la base légale de l'intérêt public de l'article 6 (1) (e) du RGPD soit plus pertinente. Pour rappel, la mission d'intérêt public est une des bases légales prévues par le RGPD sur laquelle peut se fonder un traitement de données personnelles. Le recours à cette base légale se justifie en particulier pour les traitements mis en œuvre par les autorités publiques aux fins d'exécuter leurs missions.

[21] Voir en ce sens également : CNIL, *audition de Marie-Laure Denis, Présidente de la CNIL, devant la commission des lois de l'Assemblée nationale,* 8 avril 2020. *Adde* : COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE, *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë Bulletin de veille n°1*, 7 mars 2020.

[22] Voir en ce sens : EUROPEAN DATA PROTECTION BOARD, Guidelines 04/2020, paragraphe 26 p.7, *op. cit*.

Une application qui s'insère dans des contrôles institutionnels et démocratiques

Le Conseil considère que les différents niveaux d'audit et de débat apportent les garanties de contrôles démocratiques *a priori* et *a posteriori* :

- **le premier niveau de contrôle est assuré par les entités administratives compétentes comme la CNIL qui a été officiellement saisie[23], l'Agence nationale de la sécurité des systèmes d'information (ANSSI)** qui est associée aux travaux de l'INRIA, le Comité national pilote d'éthique du numérique qui a rendu des recommandations sur le suivi des personnes par des outils numériques[24] ou encore le Comité européen de la protection des données qui a publié le 21 avril 2020 des lignes directrices sur l'utilisation des données de localisation et de contact et les outils de traçage dans le contexte de l'épidémie de COVID-19[25] ;
- **le deuxième niveau de protection est le fait que l'application sera soumise à un débat et un vote parlementaires** qui pourraient être suivis de la **mise en place d'un comité de contrôle, avec des parlementaires, des chercheurs et des citoyens-experts, disposant d'un pouvoir d'arrêt de l'application** ;
- **le troisième niveau de contrôle est celui assuré par les associations de protection des droits et des libertés, la communauté technique et académique et les médias**.

Des garanties fortes en matière de cybersécurité, gages de confiance

Afin d'offrir des garanties en matière de cybersécurité, l'application devrait se conformer aux règles de l'art en matière de cryptographie et de cybersécurité. **Le Conseil salue le fait que l'ANSSI ait été associé dès le départ aux travaux de l'INRIA**, qui pilote le développement de l'application[26].

Une ouverture du code du système, autre gage de confiance

Afin de garantir leur équité, leur responsabilité et, plus largement, leur respect des législations, **les algorithmes de l'application doivent être audités par des experts indépendants**. Le Conseil souhaite dès lors saluer l'engagement du secrétaire d'État chargé du Numérique à **rendre public le code source de l'application, des serveurs[27] et la documentation afférente sous des licences libres**, dans une démarche salutaire de transparence. Mais au-delà de la publication du code source, **il conviendra de veiller à l'intelligibilité du fonctionnement de l'application en publiant des éléments de vulgarisation compréhensibles par tous**.

---

[23] Voir : CNIL, *Crise sanitaire : audition de Marie-Laure DENIS, Présidente de la CNIL, devant la commission des lois de l'Assemblée nationale le 8 avril 2020*. La CNIL devrait rendre son avis sur l'application StopCovid avant le débat parlementaire du 28 avril 2020.

[24] COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE, *op. cit.*

[25] EUROPEAN DATA PROTECTION BOARD, Guidelines 04/2020, *op. cit*.

[26] INRIA, «"Contact tracing" : Bruno Sportisse, PDG d'Inria, donne quelques éléments pour mieux comprendre les enjeux», *op. cit.*

[27] Ce point a été précisé lors des auditions.

Comment déployer l'application en toute confiance ?

Comment se déclare-t-on infecté par le COVID-19 dans StopCOVID ?

Lorsqu'un utilisateur est testé positif au COVID-19, celui-ci devrait se déclarer dans StopCOVID. Cependant, si aucun contrôle n'est réalisé, **un utilisateur sain, mais mal intentionné pourrait se déclarer positif** pour alerter les personnes qu'il a rencontrées. **Une solution consiste à ne permettre à un utilisateur de se déclarer infecté dans l'application qu'après avoir entré une clef qui lui serait donnée par le laboratoire médical l'ayant testé**. Elle nécessite néanmoins des garanties d'anonymat pour être compatible avec les objectifs précédemment énoncés.

Quelles sont les instructions lorsqu'un utilisateur reçoit une notification ?

La procédure lorsqu'un utilisateur est notifié de son contact « à risque » avec un autre utilisateur n'a pour l'instant pas encore été communiquée. Toutefois, **cette étape peut être une source d'angoisse pour de nombreux citoyens craignant d'être infectés**. À tout le moins, **la possibilité d'un contact humain est nécessaire** (par exemple grâce à une ligne d'appel gratuite dédiée). Il conviendra cependant de **clarifier les instructions qui seront données** : doit-on se mettre en quarantaine, se faire dépister ou évaluer son exposition au risque lors des deux dernières semaines ?

Quelle sera la place de StopCOVID dans la stratégie post-confinement ?

La question de la stratégie post-confinement dépasse largement StopCOVID ; cependant, la **fracture numérique** pourrait justifier la **mise en place de stratégies différenciées en fonction des publics** (les mineurs, les personnes âgées, les exclus du numérique, etc.) avec des ressources supplémentaires **pour pallier l'impossibilité de ces publics à utiliser StopCOVID** (plus de traçage humain, par exemple).

Quels seront les critères utilisés pour évaluer l'efficacité de StopCOVID ?

Les nombreuses inconnues relatives à l'efficacité des applications de traçage de contacts, et leur inefficacité potentielle (parce que pas assez installées, pas compatibles avec tous les smartphones, pas assez précises, etc.) impliquent de **définir précisément des critères d'évaluation de l'application**. **Si ceux-ci ne sont pas remplis, les ressources humaines et financières mobilisées sur cet outil devraient être redirigées vers d'autres volets de la stratégie post-confinement**.

Les choix techniques soulèvent des controverses

Efficacité sans une masse critique d'utilisateurs

Plusieurs publications[28] sont récemment revenues sur le lien entre l'efficacité de l'application et son nombre d'utilisateurs, en évoquant l'existence d'un seuil à partir duquel elle serait suffisamment efficace pour endiguer la pandémie. **Les épidémiologistes auditionnés[29] estiment que l'application apportera toujours des bénéfices, car même sans atteindre un seuil critique d'utilisateurs, l'application peut avoir une utilité au sein de l'ensemble des mesures de post-confinement. Le Conseil considère que réduire la tension autour de la question du seuil serait alors de nature à favoriser son usage.**

La question qui se pose est alors la suivante : dans l'hypothèse où les seuils garantissant l'efficacité de l'application seule ne sont pas atteints, une faible efficacité justifie-t-elle l'investissement en temps, ressources humaines et coûts financiers ? Cette difficile évaluation d'un choix de politique publique est indispensable à l'appréciation de la pertinence de l'application.

L'obtention d'une masse critique d'utilisateurs dépend de plusieurs facteurs, tels que l'acceptabilité sociale de l'application et la communication dont elle sera entourée, qui influenceront son appropriation par la population, mais également l'émergence d'un consensus national autour d'un outil unique, afin d'éviter la multiplication des applications et la dispersion des efforts.

Cependant, certains experts voient dans le fait que l'application soit basée sur le volontariat une contrainte préjudiciable à son usage à large échelle, nonobstant tous les problèmes éthiques et juridiques qu'une obligation d'installation porterait. **Il est important de souligner que le caractère obligatoire de l'application nécessiterait une disposition législative et devrait, en tout état de cause, démontrer sa nécessité pour répondre à la crise sanitaire, son caractère circonscrit dans le temps ainsi que sa proportionnalité en tenant compte des mêmes principes de protection de la vie privée[30]**.

Précision du Bluetooth pour mesurer les distances

Dans les applications d'historique de proximité, la technologie *Bluetooth* est utilisée pour mesurer les distances entre les utilisateurs. La capacité du *Bluetooth* à mesurer précisément cette distance est encore un sujet de recherche au sein de la communauté scientifique, car cette technologie n'a pas été conçue dans ce but[31].

---

[28] Voir notamment : FERRETTI Luca, WYMANT Chris, KENDALL Michelle, ZHAO Lele, NURTAY Anel, ABELER-DORNER Lucie, PARKER Michael, BONSALL David, and FRASER Christophe, "Digital contact tracing for SARS-COV-2", Shiny app. [Consulté le 22 avril 2020].

[29] *Cf.* liste des personnes auditionnées en annexe.

[30] CNIL, *audition de Marie-Laure Denis, Présidente de la CNIL, devant la commission des lois de l'Assemblée nationale*, 8 avril 2020.

[31] LIU Shu, JIANG Yingxin, and STRIEGEL Aaron, "Face-to-face proximity estimation using bluetooth on smartphones," *IEEE Transactions on Mobile Computing*, vol. 13, no. 4, pp. 811–823, 2014.

De plus, quelle que soit son ingéniosité, le système devra, *in fine*, déduire si une rencontre avec un autre utilisateur doit être catégorisée comme à risque uniquement à partir des distances estimées par le *Bluetooth* et la durée de la rencontre. **La capacité d'opérer précisément cette catégorisation n'est pas encore avérée et sera un facteur de réussite important de l'application**[32].

Enfin, pour que l'efficacité de l'application soit optimale, il faut qu'elle soit en mesure d'enregistrer le plus de contacts possible, malgré l'accès contraint aux fonctionnalités *Bluetooth*[33] sur une part importante de smartphones, pour des raisons d'économie d'énergie et pour en éviter les mésusages. L'existence de cette limitation sur les iPhone a conduit le secrétaire d'État chargé du Numérique à demander publiquement à Apple de ne pas appliquer cette restriction à StopCOVID. Dans ses lignes directrices précitées, le Comité européen de la protection des données soutient que les deux approches (centralisée/décentralisée) sont des options viables, à condition que des mesures de sécurité adéquates soient mises en place[34].

Le déploiement doit tenir compte des contraintes du terrain

La société numérique a des angles morts

Une partie de la population est éloignée, voire exclue, du numérique[35], et la mise à disposition de solutions numériques qui lui échappe risque de renforcer la fracture à laquelle elle doit faire face**.** Souvent, **ces personnes, au premier rang desquelles les personnes âgées et les personnes en situation de précarité, sont également les plus vulnérables vis-à-vis du COVID-19**, et il existe alors un risque que l'application manque sa cible.

Un « volontariat » potentiellement contraint

Le volontariat des citoyens à l'installation et à l'utilisation de l'application peut faire l'objet d'une pression directe (en y conditionnant l'accès à un restaurant ou un cinéma par exemple) **ou sociale** (par les pairs, la cellule familiale, l'employeur, le gouvernement ou les médias) distillant l'idée que ne pas avoir l'application serait une faute. **Il en résulte un risque de conduire des citoyens non consentants à se sentir obligés d'installer l'application**. Dès lors, il convient de s'assurer que le téléchargement et l'utilisation de l'application soient effectivement basés sur un volontariat réel, avec un consentement libre et éclairé - et que le refus d'utiliser l'application n'ait aucune conséquence (accès à des lieux publics…).

POINT D'ATTENTION

[32] Même si des faux-positifs sont acceptables en vertu du principe de précaution.
[33] Voir par exemple BECHADE Corentin, «StopCovid : le Bluetooth, une technologie de "contact tracing" bancale», *Les Numériques*, 21 avril 2020.
[34] EUROPEAN DATA PROTECTION BOARD, Guidelines 04/2020, paragraphe 42, *op. cit*.
[35] LABO SOCIÉTÉ NUMÉRIQUE, *Baromètre du numérique 2019 : principaux résultats*, publié par la mission Société numérique, 28 novembre 2019.

Comment encadrer les usages dans le contexte professionnel ?

Une telle application, inscrite dans un ensemble d'autres mesures, permet potentiellement à l'employeur de satisfaire à son obligation de sécurité, de résultat et de prévention de la santé des salariés. Des usages spécifiques pourraient alors se déployer dans le contexte professionnel. Il importe qu'ils soient consentis et concertés. Il convient donc d'accompagner et d'encadrer ces usages en faisant émerger des bonnes pratiques, en accord avec les partenaires sociaux. Ces usages devraient s'insérer par ailleurs dans un cadre juridique qui permet de concilier obligations de l'employeur et droits des salariés, notamment en ce qui concerne les données personnelles[36]. La question de la validité du volontariat et du consentement relatif à l'application en milieu professionnel se pose dès lors à double titre : d'une part, en raison du lien de subordination et, d'autre part, en raison de la pression sociale. Plus largement, l'employeur ne devra pas faire de l'usage de l'application un outil de discrimination.

Entre confiance et défiance

Plusieurs risques sont spécifiquement liés à de potentiels détournements de l'application par l'État. Le développement de l'application risque de **démocratiser une emprise numérique sur les comportements, et d'engendrer une défiance envers l'État (perçu comme trop intrusif) ou, *a contrario*, de pérenniser et banaliser certaines formes de suivi numériques.** Un potentiel conditionnement de la sortie du confinement ou de l'accès à certains espaces à l'utilisation de l'application serait également dommageable et briserait la logique de consentement des usagers.

Un impact sur les pratiques sociales difficile à prévoir

Enfin, on peut identifier des risques touchant directement la population, allant de **la procuration d'un faux sentiment de protection lorsque l'application est installée au développement d'un climat anxiogène, de méfiance, de discrimination sociale, voire de stigmatisation, envers les autres citoyens.**

Communiquer au milieu d'un débat passionnel

Les différents enjeux soulevés précédemment appellent une **communication soigneusement réfléchie par le Gouvernement et ses partenaires lors du lancement de l'application**, le contexte de crise sanitaire accentuant les réactions passionnelles et la diffusion de fausses nouvelles.

L'acceptabilité sociale n'est pas acquise. Pour répondre aux interrogations et aux craintes des citoyens vis-à-vis de l'application, créer un esprit de confiance et mobiliser les citoyens autour de cet outil, **la parole**

[36] Voir notamment : BLANDIN Annie, « Les données personnelles au cœur des rapports entre employeur et travailleur. L'enjeu de sécurité », *Études digitales*, n°2, oct 2017.

publique doit être clairement structurée, transparente et étayée par la Science et le Droit. Il en va de l'acceptabilité de l'application, de son adoption et, en conséquence, de son degré d'utilité.

CONTROVERSE	
Les acteurs de la médiation numérique doivent-ils être mobilisés comme *« ambassadeurs »* de l'application auprès des citoyens ?	
Pour	Contre
Leur maillage du territoire et leur connaissance du terrain et des publics éloignés du numérique sont des atouts à mobiliser pour créer de la confiance et réaliser des actions de pédagogie au sein de la population.	Leur rôle n'est pas là et les efforts de communication doivent essentiellement être portés par l'aide sociale, la communauté médicale et les pouvoirs publics.

En pleine crise, la souveraineté numérique reste un enjeu clef

Le Conseil considère que la France, comme les autres pays européens, doit garder le choix du fonctionnement de l'application d'historique de proximité. Le bras de fer qui oppose actuellement les gouvernements aux fournisseurs de systèmes d'exploitation mobiles[37] sur l'accès aux fonctionnalités *Bluetooth* met en lumière l'importance de la maîtrise de la souveraineté autour des outils numériques (et des applications d'historique de proximité).

Les choix de santé publique doivent être du ressort de la puissance publique

Apple et Google se sont proposés d'aider les gouvernements dans le développement de solutions d'historique de proximité. **Alors que la caractérisation des contacts pertinents[38] se fait au niveau national au sein des comités scientifiques, les briques logicielles proposées par les deux géants contraignent les possibilités de calibrage de la caractérisation des contacts**. Cette solution technique a un impact sur la maîtrise qu'ont les gouvernements (l'algorithme de la solution étant une composante de la politique publique) et du choix de l'architecture de l'application (centralisée ou décentralisée). Les fournisseurs de

[37] SCHMITT Fabienne, DEBES Florian, «StopCovid : Cédric O demande à Apple de « lever les barrières techniques »», *Les Echos*, 20 avril 2020.
[38] Les caractéristiques de qualification s'intéressent au temps d'exposition, à la distance entre deux individus, aux types de protection entre les deux individus, etc.

systèmes d'exploitation mobiles doivent respecter les choix souverains des États sans imposer ni favoriser une architecture[39] ou un algorithme précis.

« Une pour tous et tous pour une »

Des sociétés privées voulant mettre à profit leurs compétences et leurs savoir-faire développent et proposent d'ores et déjà des solutions d'historique de proximité[40]. Néanmoins, il faut éviter le morcellement dans la mise en œuvre de la stratégie sanitaire sur le territoire national. **La multiplication d'applications en France entraînerait une fragmentation du dispositif qui pourrait nuire à son efficacité**. Il serait plus opportun d'associer les sociétés privées volontaires au développement d'autres outils numériques utiles dans le cadre de la crise du COVID-19.

Jusqu'où pousser la coopération internationale et européenne ?

Alors que les échanges avec les entreprises extraeuropéennes peuvent être perçus comme des luttes de pouvoir, la coopération scientifique internationale et européenne reste un élément important dans le développement d'un outil numérique, tant pour l'échange d'informations que pour la validation des protocoles et des dispositifs scientifiques. Cependant, une application européenne unique (ou dans une moindre mesure des applications interopérables) déplacerait la finalité vers la libre-circulation au sein de l'Union européenne et présente le risque de **conditionner l'arrêt de l'application au contrôle de l'épidémie dans l'ensemble des territoires des États membres**.

CONTROVERSE	
Faut-il promouvoir l'interopérabilité des applications en Europe ?	
Pour	Contre
Sans l'émergence d'une application unique ou sans interopérabilité des applications, la question des citoyens transfrontaliers ne pourrait être facilement résolue.	Une solution européenne, ou une interopérabilité des solutions européennes contraindrait l'arrêt de l'application à un contrôle de l'épidémie chez tous les États membres alors que les effets de la crise ne sont pas homogènes au sein de l'Union.

[39] *Cf. supra :* le Comité européen de la protection des données a mis en avant que les deux architectures pouvaient être des options viables pour la protection des données, à condition que des mesures de sécurité adéquates soient en place.
[40] BALENIERI Raphaël,«GODELUCK Solveig, DEBES Florian, « Appli StopCovid : le terrain s'impatiente», *Le Parisien*, 21 avril 2020.

Annexe – Lettre de saisine

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'ECONOMIE
ET DES FINANCES

MINISTERE DE L'ACTION
ET DES COMPTES PUBLICS

SECRETARIAT D'ETAT
CHARGE DU NUMERIQUE

Le Secrétaire d'Etat

Paris, le 14 avril 2020

Objet : lettre de saisine sur le projet StopCOVID

Madame la Présidente,

Le Ministre des Solidarités et de la Santé et moi-même avons récemment annoncé le développement d'un prototype d'application de reconstitution de l'historique de proximité « StopCOVID », dans le but d'aider à identifier rapidement les chaînes de contamination potentielle. Comme le rappelle le Conseil Scientifique COVID-19 dans son avis du 2 avril 2020[1], il est crucial de commencer le développement d'un tel dispositif dans l'hypothèse où il pourrait se révéler utile dans une étape postérieure de gestion de l'épidémie, parmi d'autres mesures sanitaires.

Le projet « StopCOVID » entend respecter pleinement les cadres légaux français et européen de protection des libertés, notamment le Règlement Général de Protection des Données. Il est fondé sur une installation volontaire de l'application et une anonymisation des données, de telle manière que personne ne puisse être capable ni de retracer la liste des personnes testées positives ni, le cas échéant, de reconstituer qui a contaminé qui. Le gouvernement veille à associer la CNIL au travail du projet « Stop COVID ». Les spécifications de l'application lui seront soumises. Le projet est destiné à être open source, c'est-à-dire que le code de l'application sera rendu public et que n'importe qui pourra prendre connaissance de ses principes de fonctionnement.

Madame Salwa TOKO
Présidente du Conseil national du numérique
6 rue Louise Weiss
75013 PARIS

[1] « Le gouvernement devra s'assurer que les éléments d'une stratégie postconfinement seront opérationnels, incluant notamment : […] de nouveaux outils numériques permettant de renforcer l'efficacité du contrôle sanitaire de l'épidémie » https://solidarites-sante.gouv.fr/IMG/pdf/avis_conseil_scientifique_2_avril_2020.pdf

Pleinement conscients des questions légitimes que la mise en place d'une telle application pourrait susciter, nous souhaitons poursuivre notre démarche de transparence, qui nous l'espérons, permettra une adhésion forte du citoyen dans un outil qui doit participer à sa protection et à celle de tous.

Aussi, je souhaite pouvoir m'appuyer sur l'expertise du Conseil national du numérique pour enrichir nos réflexions sur le déploiement de l'application « StopCOVID », dans la mesure où celle-ci serait retenue dans une stratégie sanitaire d'allègement du confinement, en conformité avec les obligations sanitaires associées. Vous me ferez part des points d'attention, des améliorations possibles qui vous auront été signalées lors de vos auditions. Vous ferez des recommandations sur les conditions qui pourraient permettre son adoption par le plus grand nombre et notamment sur la question essentielle de l'inclusion.

Pour bâtir votre avis, vous pourrez rencontrer les acteurs pertinents de la société civile, des entreprises et de la recherche, en France ou à l'étranger. Vous veillerez à coordonner vos travaux avec ceux de la *task force* créée pour le développement du prototype d'application et me rendrez vos conclusions au plus tard le 24 avril 2020.

Je vous prie d'agréer, Madame la Présidente, l'expression de ma considération distinguée.

Cédric O

La lettre de saisine est aussi disponible sur le site web du Conseil.

Annexe — Liste des auditions et contributions

Contributions écrites

- Didier Fassin, sociologue, membre du Collège de France
- Loïc Gervais, médiateur numérique, contribution disponible en ligne
- Alain Giffard, ancien président de la Mission Interministérielle pour l'accès public à l'Internet, contribution disponible en ligne
- Olivier Sauvage, président de l'association francophone des professionnels de l'expérience utilisateur

Personnes auditionnées

- Alexandre Archambault, avocat au barreau de Paris
- Maryse Artiguelong, membre de la Ligue des droits de l'Homme
- Serge Abiteboul, membre du collège de l'ARCEP
- Alain Barrat, directeur de recherches au CNRS
- Jérémie Boroy, président du Conseil National Consultatif des Personnes Handicapées
- Joël Chandelier, maître de conférences en histoire médiévale à l'Université Paris 8
- Marie Cohen-Skalli, directrice adjointe Emmaüs connect
- Grégoire Ducret, directeur innovation et stratégie de la Croix-Rouge Française
- Marie-Laure Denis, présidente de la CNIL
- Olivier Faure, professeur émérite d'histoire contemporaine
- Eric Fleury, directeur du centre de recherche Inria de Paris, INRIA
- Aymeril Hoang, membre du conseil scientifique sur COVID-19
- Gwendal Legrand, secrétaire général adjoint de la CNIL
- Daniel Lemetayer, directeur de recherche, INRIA
- Alexandra Mailles, médecin (Direction des maladies infectieuses), Santé Publique France
- Arthur Messaud, juriste, La Quadrature du Net
- Chiara Poletto, chargé de recherches à l'INSERM
- Vincent Roca, chef de l'équipe de recherche Privatics, INRIA
- Pierre-Louis Rolle, directeur de la mission Société numérique
- Sébastien Soriano, président de l'ARCEP
- Bruno Sportisse, président directeur général de l'INRIA
- Tom-Louis Teboul, responsable partenariats Emmaüs Connect

Liste des membres du Conseil national du numérique

Présidente
Salwa Toko

Vice-Président
Gilles BABINET

Membres
Yann ALGAN
Maud BAILLY
Annie BLANDIN-OBERNESSER
Mohammed BOUMEDIANE
Jérémie BOROY
Patrick CHAIZE
Théodore CHRISTAKIS
Olivier CLATZ
Nathalie COLLIN
Vincent COSTALAT
Maryne COTTY-ESLOUS
Karine DOGNIN-SAUZE
Gaël DUVAL
Gérald ELBAZE
Hind ELIDRISSI
Florette EYMENIER
Martine FILLEUL
Sophie FLAK
Henri ISAAC
Tatiana JAMA
Loubna KSIBI
Anne LALOU
Thomas LANDRAIN
Constance LE GRIP
Litzie MAAREK
Laura MEDJI
Françoise MERCADAL-DELASALLES
Jean-Michel MIS
Hervé PILLAUD
Jean-Charles SAMUELIAN
Christian VANIZETTE
Alexandre ZAPOLSKY

Secrétariat général
Eric BERNAVILLE, Assistant de direction

Rédacteurs
Charles-Pierre ASTOLFI, Secrétaire général
Vincent TOUBIANA, Secrétaire général adjoint
Nathalie BOUAROUR, rapporteure
Marylou LE ROY, responsable juridique et des affaires institutionnelles
Jean-Baptiste MANENTI, rapporteur

Relectures
Leila AMANAR, rapporteure
Myriam EL ANDALOUSSI, rapporteure
Joséphine HURSTEL, rapporteure alternante
Ménéhould MICHAUD DE BRISIS, rapporteure
Philippine REGNIEZ, rapporteure
Hugo BESANCON, stagiaire
Farah FEJJARI, stagiaire

À propos du Conseil national du numérique

Le Conseil national du numérique est une commission consultative indépendante. Il est chargé d'étudier les questions relatives au numérique, en particulier les enjeux et les perspectives de la transition numérique de la société, de l'économie, des organisations, de l'action publique et des territoires.

Il est placé auprès du ministre chargé du numérique. Ses statuts ont été modifiés par décret du 8 décembre 2017. Ses membres sont nommés par arrêté du Secrétaire d'État chargé du numérique pour une durée de deux ans.

Contact presse
Charles-Pierre Astolfi — Secrétaire général
presse@cnnumerique.fr
01 44 97 25 00
https://cnnumerique.fr | @CNNum