Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONSEIL NATIONAL DU NUMÉRIQUE

À Paris, le 7 juillet 2017

Monsieur le Ministre,

Le Conseil national du numérique est une commission consultative indépendante composée de 30 membres nommés par le Président de la République et chargés d'éclairer le Gouvernement sur l'impact des technologies numériques sur la société et l'économie. En ce début de quinquennat, il nous apparaît important de prendre contact avec vous afin de vous proposer une collaboration utile sur la question du délicat équilibre entre libertés et sécurité.

Cette question se pose avec acuité en matière de chiffrement des données. Dans une déclaration commune avec la Première ministre britannique Theresa May, le président de la République Emmanuel Macron s'est une nouvelle fois prononcé en faveur d'un meilleur accès aux contenus chiffrés, « *dans des conditions qui préservent la confidentialité des correspondances, afin que [les] messageries ne puissent pas être l'outil des terroristes ou des criminels* ». Le Conseil a déjà eu l'occasion de s'exprimer sur cette question et il rendra un avis détaillant sa position sur le sujet dans le courant de l'été. En substance, il considère que **le chiffrement est un outil vital pour la sécurité en ligne.** Les technologies de chiffrement font partie du domaine public : partant, toute tentative visant à en limiter l'accès pour le grand public reviendrait à en accorder le monopole aux organisations criminelles qui sauront en abuser.

Plus généralement, le Conseil est particulièrement préoccupé par la trajectoire sécuritaire opérée ces dernières années, en particulier sur le numérique et les réseaux d'échange. Dans le discours politique, ces derniers apparaissent bien souvent comme des « coupables idéaux ». Ainsi servent-ils généralement de terrain d'expérimentation pour le déploiement dans le droit commun des instruments sécuritaires, l'opinion publique s'accommodant plus facilement d'une surveillance en ligne globalement considérée comme moins intrusive. S'il n'est pas question de nier le rôle déterminant du numérique dans les processus de radicalisation et l'organisation des réseaux terroristes, cette responsabilité est beaucoup plus complexe qu'il n'y paraît et le contact humain reste un déclencheur majeur du processus de radicalisation.

Cette trajectoire sécuritaire, dans laquelle semble s'inscrire le projet de loi *renforçant la lutte contre le terrorisme et la sécurité intérieure*, entérine une logique du soupçon dans le droit commun. Au nom d'une conception prédictive de la lutte antiterroriste, des individus pourraient être contraints non parce qu'ils prépareraient des crimes ou des délits, mais parce qu'ils seraient susceptibles d'en commettre (ou car on soupçonnerait leur adhésion à des thèses extrémistes).

Monsieur Gérard COLLOMB,
Ministère de l'Intérieur,
Place Beauvau
75800 Paris Cedex 08

CNNum
Conseil National du Numérique

Bâtiment Atrium – 5 Place des Vins de France 75572 Paris cedex 12
Contact : tél. 01 53 44 21 27 - mél. info@cnnumerique.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Le Conseil s'inquiète par ailleurs d'un amenuisement progressif de l'autorité judiciaire au bénéfice de l'autorité administrative. Bien sûr, il n'est pas question de nier l'importance du contrôle du juge administratif et son rôle historique dans la préservation des libertés individuelles. Néanmoins, ce contrôle intervient nécessairement après la mise en cause d'une liberté et suppose la saisine préalable du juge administratif — ce qui en pratique n'arrive que très rarement.

Conscient de la criticité des menaces qui pèsent sur notre pays, le Conseil n'entend pas moins assurer son rôle de vigie dans la préservation de l'État de droit. L'ampleur des transformations induites par le numérique devrait nous imposer une réflexion globale et collective plutôt qu'un empilement de mesures, parfois prises dans l'urgence et sous le coup de l'émotion. Le Conseil souhaite accompagner votre ministère dans la détermination de ces équilibres, afin de renforcer le niveau de sécurité de nos concitoyens sans rogner sur le respect des libertés individuelles et collectives.

Sur un autre sujet, **le Conseil tient par ailleurs à réaffirmer ses préoccupations quant au déploiement du fichier des *"Titres électroniques sécurisés"* (TES)**, censé contenir à terme les données biométriques de la quasi-totalité de la population française. Dans un contexte où les fuites de données sont légion et les attaques informatiques de plus en plus redoutables, la centralisation de ces données sensibles soulève des inquiétudes légitimes. Les conclusions de l'audit mené par l'ANSSI et la DINSIC nous apparaissent en outre incompatibles avec une généralisation à la hâte du système TES, compte tenu des réserves importantes exprimées par la mission. *A minima*, nous vous invitons à expliciter le plan d'action correspondant aux 11 recommandations d'évolution listées dans son rapport. Compte tenu des réserves importantes exprimées par la mission, elles devraient conduire le Gouvernement à séparer les deux sujets que sont la mise en place du fichier TES de l'implémentation du Plan Préfecture Nouvelle Génération (PPNG). Si le calendrier du plan de modernisation des préfectures n'est pas à remettre en cause, l'authentification biométrique pour la délivrance des cartes d'identité n'en est pas un élément indispensable. Comme cela avait été souligné dans l'avis du CNNum, le rapport d'audit mentionne en effet que "*la centralisation des données biométriques pour la carte nationale d'identité n'a pas actuellement un intérêt direct pour leur gestion. Leur utilisation se borne en effet au cas des réquisitions judiciaires*".

Plus largement, la polémique qui a entouré le fichier TES est à notre sens révélatrice d'une difficulté plus structurelle : l'État et ses organes doivent poursuivre leur adaptation afin de prendre les meilleures décisions technologiques possibles au regard, notamment, de leurs implications politiques, économiques et sociétales. Ici encore, notre Conseil souhaite vivement pouvoir accompagner l'action de votre ministère.

Nous vous prions de croire, Monsieur le Ministre, à l'assurance de nos sentiments les meilleurs.

Guy MAMOU-MANI,
Vice-Président du CNNum

Sophie PENE,
Vice-Présidente du CNNum

Amal TALEB,
Vice-Présidente du CNNum

CNNum
Conseil National du Numérique

Bâtiment Atrium – 5 Place des Vins de France 75572 Paris cedex 12
Contact : tél. 01 53 44 21 27 - mél. info@cnnumerique.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Conseil national du numérique - Juillet 2017

Note thématique - 3 sujets liés à la sécurité des citoyens français

Le Conseil national du numérique (CNNum) est une Commission consultative indépendante chargée de formuler des avis et recommandations publiques sur toute question relative à l'impact du numérique sur la société et sur l'économie. Ses membres bénévoles sont issus de la société civile et nommés par le président de la République. Il joue auprès du gouvernement le rôle de conseil stratégique et celui d'interface pour les écosystèmes de la société numérique.

Ce document est destiné à faciliter la mise à profit de l'expertise du CNNum par la nouvelle équipe gouvernementale. Il propose à cette fin 3 sujets au coeur de l'équilibre entre la sécurité des citoyens français et des droits et libertés dans un monde instable sur lesquelles le Conseil pourrait être sollicité dans les prochains mois. Ces sujets correspondent soit à des mesures spécifiques contenues dans le programme politique du président de la République ; soit à des enjeux qui nous semblent fortement liés à sa philosophie générale telle que nous l'avons comprise :

1. Engager un dialogue sur les équilibres à trouver dans le cadre de la lutte antiterroriste, notamment concernant le chiffrement

Le Conseil a eu l'occasion de s'exprimer de nombreuses fois sur la question du chiffrement. Il s'agit avant tout d'un outil de protection vital face à des cybermenaces toujours plus redoutables. Pour le citoyen, il est le levier majeur de la confiance dans l'univers numérique. Pour les entreprises, il est aujourd'hui le meilleur rempart contre l'espionnage économique. Pour l'État, le chiffrement des données participe à la préservation de notre souveraineté.

Une limitation du chiffrement aboutirait à un affaiblissement dommageable de la sécurité sur l'ensemble des réseaux. Par ailleurs, de telles mesures auraient une efficacité toute relative sur l'infime minorité d'utilisateurs ciblés. Publiques et largement diffusées, les technologies de cryptographie sont aujourd'hui à la portée de n'importe quelle organisation criminelle. Limiter le chiffrement pour le grand public reviendrait alors à en accorder le monopole aux organisations qui sauront en abuser.

Sans nier le fait qu'il puisse compliquer l'accès à certaines informations, le chiffrement ne constitue pas une barrière infranchissable pour la résolution des enquêtes. D'une part, il est souvent possible de le contourner, même s'il est très robuste, en exploitant des failles techniques ou en s'introduisant directement dans l'équipement de la personne ciblée. D'autre part, les métadonnées restent le plus souvent en clair et permettent de répondre à des questions importantes sur le comportement d'une personne.

2. S'interroger sur la place de l'autorité judiciaire dans le contrôle des mesures de surveillance

Bâtiment Atrium – 5 Place des Vins de France 75572 Paris cedex 12
Contact : tél. 01 53 44 21 27 - mél. info@cnnumerique.fr

Le Conseil a toujours soutenu la nécessité de porter une attention particulière au contrôle des techniques de surveillance. En effet, face à la montée en puissance des acteurs de la sécurité, il est de notre responsabilité de constamment nous interroger sur l'équilibre entre les pouvoirs et les devoirs des services de renseignement. Si les services ont accès à de plus en plus d'information, il n'est pas anormal que leurs devoirs et leur contrôle augmentent en conséquence.

Par ailleurs, le Conseil a également invité à renforcer les garanties et les moyens du contrôle démocratique. En plus d'un contrôle opéré au cas par cas, il est impératif qu'une autorité puisse s'assurer de l'efficacité et de la stricte proportionnalité du dispositif global par rapport aux objectifs poursuivis.

3. Ouvrir une réflexion publique et globale sur l'identité à l'heure du numérique

Les sujets de l'identité administrative et de l'identité numériques sont traités séparément en France depuis plus de 10 ans. Néanmoins, la question de leur relation est appelée à prendre de l'ampleur dans les prochaines années. À court terme, il s'agit d'assurer le plus haut niveau d'interopérabilité prévue par la législation européenne et française (règlement eIDAS et loi pour une République numérique) et de tirer pleinement partie des avancées et des réflexions de la recherche. À long terme, il est question de penser un modèle pour notre société numérique. Il semble en particulier nécessaire de développer une réflexion sur les impacts profonds sur notre société d'une généralisation des procédures d'authentification pour accéder à tout service - public ou privé, en France ou à l'étranger. Il s'agit d'un chantier multidisciplinaire de grande ampleur et essentiel à la construction de notre pays, qui ne peut être éludé par des prises de décisions qui répondent uniquement à des besoins opérationnels immédiats. Nous devons en effet nous questionner au préalable sur les visions sociale, politique, philosophique et économique de l'identité à l'ère numérique.

Bâtiment Atrium – 5 Place des Vins de France 75572 Paris cedex 12
Contact : tél. 01 53 44 21 27 - mél. info@cnnumerique.fr