CONSEIL NATIONAL DU NUMÉRIQUE

COMMUNIQUÉ DE PRESSE

Fichier TES : le CNNum appelle le Gouvernement à suspendre sa mise œuvre et s'autosaisit pour examiner des alternatives techniques plus modernes et respectueuses des droits et libertés

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CNNum
Conseil National du Numérique

Contact presse

Yann Bonnet
Secrétaire général
presse@cnnumerique.fr
01 53 44 21 27

www.cnnumerique.fr
@cnnum

PARIS — Le dimanche 30 octobre, le Gouvernement a publié le décret n°2016-1460 prévoyant l'instauration d'un nouveau fichier des "titres électroniques sécurisés" (TES) à l'ampleur inégalée. Ce dernier vise à élargir le fichier TES, qui existe déjà pour la gestion des passeports biométriques, aux cartes d'identités. Présenté comme un moyen de lutte contre la fraude documentaire, ce fichier pourra néanmoins faire l'objet de réquisitions judiciaires ou être utilisé par les services spécialisés de renseignement. A terme, il pourrait conserver les données biométriques de près de 60 millions de français dans une base centralisée. Cette décision administrative, prise sans aucune concertation préalable et minimisée dans ses conséquences depuis lors par le Gouvernement, suscite depuis une semaine une inquiétude croissante. Le Conseil national du numérique a donc décidé de s'autosaisir du fichier TES en vue de la publication prochaine d'un avis détaillé.

En premier lieu, le Conseil déplore l'absence de toute concertation préalable à la publication de ce décret. Un dialogue avec les communautés d'experts aurait certainement pu permettre au Gouvernement d'explorer des alternatives techniques plus résilientes et respectueuses des droits des citoyens, tout en permettant d'atteindre les mêmes objectifs. À un mois du Sommet de Paris sur le Partenariat pour un gouvernement ouvert (PGO) présidé par la France pour un an, cette opacité contraste fortement avec les objectifs affichés par les pouvoirs publics en matière de transparence, sans compter qu'elle s'inscrit à rebours de la démarche de consultation initiée par Axelle Lemaire sur les décrets d'application de la loi pour une République numérique.

L'existence de ce fichier laisse la porte ouverte à des dérives aussi probables qu'inacceptables

Le choix, pris par décret, d'une architecture technique centralisée pour la conservation de données biométriques soulève un grand nombre

d'inquiétudes. Dans un monde numérique où le code fait la loi, l'existence d'un tel fichier laisse la porte ouverte à des dérives aussi probables qu'inacceptables. Aussi légitimes que soient les finalités initiales du Gouvernement, rien ne pourra techniquement prévenir leur extension future au gré d'une grave actualité. Il suffira alors, pour le pouvoir en place, de changer quelques lignes d'un décret pris en Conseil d'État après simple avis consultatif de la CNIL (depuis 2004 l'autorité ne dispose plus de son pouvoir de veto). L'existence même d'un fichier centralisé suffit mécaniquement à susciter des appétits ; un fichier massif est propice aux détournements massifs de finalités. Ces dernières pourraient à terme permettre l'identification systématique de la population avec les moyens de la reconnaissance faciale ou de la reconnaissance d'image, à des fins policières ou administratives.

L'histoire récente nous enseigne que la constitution de tels fichiers a régulièrement conduit à l'élargissement de leurs finalités initiales, qu'ils s'opèrent dans un cadre légal (comme pour le système Eurodac des demandeurs d'asile, le fichier des demandeurs de visa ou encore le STIC) ou hors de tout contrôle (rappelons que l'absence d'encadrement était, jusqu'à une époque récente, caractéristique de l'activité des services de renseignement). Penser que notre pays ferait exception revient à ignorer les leçons de l'histoire et des comparaisons internationales. Les reculs démocratiques et la montée des populismes, observés y compris en Europe et aux États-Unis, rendent déraisonnables ces paris sur l'avenir.

Le choix de la centralisation revient à créer une cible d'une valeur inestimable

Ces menaces peuvent sembler lointaines à certains ; mais d'autres apparaîtront immédiatement dès la mise en ligne du fichier. La publication de ce décret intervient à un moment où les cybermenaces se font redoutables et où tout indique que ces risques ont changé d'échelle : rappelons que de façon inédite, l'issue des élections américaines peut en partie dépendre des conséquences de piratages d'Etats. **Dans ce contexte, le choix de la centralisation revient à créer une cible d'une valeur inestimable, face à des adversaires qui ne sont pas des amateurs.** En matière de sécurité informatique, aucun système n'est imprenable. Les défenses érigées comme des lignes Maginot finissent immanquablement par être brisées. Comme le soulignait par ailleurs Jean-Jacques Urvoas en 2012 (au sujet de la proposition de loi qui a semble-t-il inspirée ce décret), ce n'est qu'une question de temps[1].

[1] Ainsi en 2009, un registre de la population israélienne contenant des informations confidentielles sur près de 9 millions de citoyens se retrouvait sur Internet à la suite d'une négligence d'un sous-traitant. Au mois d'avril dernier, une faille de sécurité avait entraîné une fuite massive de données relatives à 55 millions d'électeurs philippins. Le même mois, c'est une base de données tirée du recensement de la population turque qui été mise en ligne, avec noms et adresses.

Les réponses juridiques doivent absolument s'accompagner de garanties techniques

À ces menaces ouvertes par la technique, les réponses juridiques ne suffisent plus : elles doivent s'accompagner de garanties techniques. Il s'agit autant de garantir la résilience du système TES à ces détournements de finalités que d'assurer la sécurité des données de nos concitoyens. Techniquement, de telles architectures existent et fondent déjà une part importante de l'économie numérique : c'est le sens du mouvement en faveur du *privacy by design* (la protection de la vie privée dès la conception). A ce titre, nombreux sont ceux à recommander la conservation des données biométriques sur un support individuel exclusivement détenu par la personne, à l'instar de la CNIL ou du Conseil constitutionnel. Cette conservation pourrait par exemple, mais ce n'est pas l'unique possibilité, s'opérer au moyen d'un composant électronique intégré aux cartes d'identité, comme c'est les cas pour les passeports.

Ces alternatives, qui s'inscrivent dans la logique d'autodétermination informationnelle consacrée par la loi numérique, permettent d'atteindre les objectifs de lutte contre la fraude documentaire tout en étant respectueuses de la vie privée des citoyens. Les balayer d'un revers de main revient — qu'on l'ait voulu ou non — à ignorer l'état actuel des technologies disponibles et à faire obstacle au progrès des droits et des capacités des individus au profit d'une mise sous tutelle de la population par ses gouvernants.

Le Conseil national du numérique contribuera ainsi à la réflexion entourant ce nouveau fichier. Dans les prochains jours, il étudiera les alternatives techniques à cette base centralisée et les garanties qui pourraient lui être apportées — toutes les personnes disposées à l'aider dans cette démarche sont invitées à prendre contact à l'adresse suivante : info@cnnumerique.fr. Dans l'intervalle, il appelle le Gouvernement à suspendre la mise en œuvre de ce fichier ainsi que la publication des arrêtés et à initier une réflexion ouverte en impliquant les experts numeriques au sein de l'Etat comme la DINSIC (Direction interministérielle du numérique et des systèmes d'information et de communication) et au sein de la société civile avec le CNNum.

Paris, le 7 novembre 2016