La nouvelle carte d'identité électronique comme support nécessaire d'une identité numérique qui tarde à être mise en œuvre…

Par Catherine Prebissy-Schnall, Maître de conférences HDR en droit public à l'Université Paris Nanterre

Par un **décret n°2021-279 du 13 mars 2021**, la France a créé une nouvelle carte nationale d'identité électronique (CNIe) qui viendra remplacer progressivement celle qui, dans sa version de 1995, est actuellement encore en circulation. Saisie pour avis (**délibération n°2021-022**), la CNIL a donné son accord au déploiement de cette carte qui est expérimentée depuis le 15 mars dans le département de l'Oise et depuis le 29 mars en Seine-Maritime et à La Réunion. Ce dispositif sera généralisé à la France entière à compter du 2 août prochain. Cette dernière date correspond à l'entrée en application du **règlement européen 2019/1157** qui impose aux États membres de l'Union européenne de mettre en circulation des cartes d'identité intégrant un composant électronique hautement sécurisé contenant des données biométriques, à savoir une image numérisée du visage du titulaire de la carte et celle des empreintes digitales de deux doigts, dans des formats numériques interopérables. L'enjeu est de mieux lutter contre la fraude documentaire et l'usurpation d'identités (45 000 plaintes déposées en 2019).

Si la France s'est ainsi pliée à la volonté européenne, 6 mois avant la date limite et donc avec un grand retard par rapport à ses voisins européens, elle était pourtant pionnière en la matière avec de nombreuses tentatives d'instauration d'une carte électronique dès 2003. Désormais, si le retard semble rattrapé, l'inquiétude porte non seulement sur les risques liés au traitement des données biométriques mais également sur l'absence de calendrier concernant la proposition d'une identité numérique régalienne pour tous les français, dérivée de la CNIe.

Quelles sont les nouveautés apportées par la CNIe et quelles garanties sont apportées pour protéger les données à caractère personnel ?

Au design modernisé avec des éléments en relief pour les personnes malvoyantes, cette carte dispose d'un cachet électronique visible contenant des données signées du titulaire et garantissant l'authenticité du titre. Facultative et gratuite, elle est produite par l'imprimerie nationale pour une durée de validité de 10 ans. À compter d'août 2031, les anciennes cartes ne permettront plus de voyager dans les autres pays européens mais pourront toujours servir pour justifier de son identité. Pour les personnes détenues ou dans l'incapacité physique de se déplacer, les agents de préfecture ou de mairies pourront prendre des photographies avec un dispositif de recueil mobile.

Les données biométriques du titulaire sont logées dans une puce très sécurisée dont la lecture automatique est possible lors des contrôles par les forces de l'ordre et lors des passages aux points de contrôle des aéroports, des gares et des ports au sein de l'UE. Bien que les données biométriques figurent déjà dans la puce « infalsifiable » insérée dans la carte, elles sont également traitées dans la base centralisée TES (titres électroniques sécurisés) qui réunit depuis 5 ans les données biométriques des passeports électroniques et des cartes d'identité de près de l'ensemble de la population française et dont le ministère de l'Intérieur et l'Agence nationale des titres sécurisés (ANTS) sont responsables conjointement. Ce traitement permet de procéder à la comparaison automatique des empreintes digitales du demandeur avec celles précédemment enregistrées sous la même identité à des fins d'authentification. Si le Conseil d'État a validé cette base de données (**CE, 18 oct. 2018, n°404996**), l'encadrement de son utilisation reste soumis à une vigilance renforcée de la part de la CNIL qui n'a jamais approuvé ce choix technologique (non retenu en Belgique et en Allemagne). En effet, avec cette nouvelle extension aux données biométriques recueillies par la nouvelle carte, la dimension incroyable de ce fichier va susciter toutes les convoitises (cyber-attaques, usages multiples) d'autant que le décret a prévu deux modifications majeures : au titre de la nouvelle finalité de lutte contre l'usurpation d'identité, une

transmission des données du traitement TES va s'opérer vers le fichier national de contrôle de la validité des titres (DOCVERIF) et vers les logiciels de rédaction des procédures de la police et de la gendarmerie en cas de déclaration de vol de titre. Au titre du respect de l'exigence européenne, le recueil des empreintes est désormais obligatoire (sauf pour les mineurs de moins de douze ans) avec une durée de conservation de 15 ans dans la base centrale (contre seulement 90 jours en Allemagne).

Toutefois, le demandeur peut refuser que l'image numérisée de ses empreintes soit conservée dans la base de données TES (titres électroniques sécurisés) au-delà d'un délai de 90 jours à compter de la date de délivrance du titre. Dans ce cas, une copie sur papier est conservée pendant 15 ans par les agents habilités et toute consultation de cette copie fait l'objet d'une traçabilité. Par ailleurs, le traitement TES ne peut être utilisé que dans un processus d'authentification mais ne peut en aucun cas, ni juridiquement ni techniquement, être utilisé dans un processus d'identification (à partir d'une empreinte, on ne peut pas remonter à une identité).

La crainte que la CNIe entrouvre la porte d'un régime orwellien n'est donc pas fondée dans la mesure où des garanties de protection des données à caractère personnel conformes au RGPD sont apportées.

Pourquoi la France se dote-elle si tardivement de la CNIe ?

En France, une polémique de grande ampleur est née en 1973 à travers l'informatisation du répertoire des numéros tenu par l'INSEE sous le nom de projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus). Considéré comme une manœuvre secrète du gouvernement pour ficher chaque français, le projet a été abandonné et la **loi informatique et libertés du 6 janvier 1978** adoptée avec la naissance de la CNIL. Il reste cependant que l'ombre de cette affaire a continué de planer et est venue assombrir tous les projets d'identification mobilisant les données d'identité : seules les cartes d'identité électroniques professionnelles comme la carte CPS pour

les professionnels de santé ont pu voir le jour dès la fin des années 1990. Depuis les événements du 11 septembre 2001 et face à la recrudescence des fraudes à l'identité, pas moins de cinq projets de modernisation de la carte d'identité ont été lancés (comme le programme INES en 2005 – Identité Nationale Électronique Sécurisée – ou le projet Idénum en 2010) mais sans succès. Face à ces échecs et en réponse aux problèmes techniques posés par la numérisation des services publics, le gouvernement a abandonné l'idée de création d'une identité numérique régalienne corrélée à un titre électronique et a décidé de créer en 2014 le dispositif FranceConnect qui se développe comme un fédérateur d'identités (au pluriel) puisqu'il agit comme un tiers de confiance pour authentifier un usager qui souhaite accéder à d'autres services que ceux pour lesquels il dispose déjà d'identités numériques. L'objectif recherché est que l'usage de ce fédérateur d'identité garanti par l'État s'impose et prévaut sur toute autre procédé d'identification proposé par les GAFAM. Le choix technologique de l'État aurait pu être différent et s'appuyer notamment sur la mise en place de la carte nationale d'identité électronique dont les bases de la création étaient déjà posées par la **loi du 27 mars 2012 relative à la protection de l'identité**. Mais la volonté politique a été précisément d'éviter de mobiliser cette carte dans les pratiques d'identification compte tenu du contexte de suspicion à l'égard de la multiplication des fichiers nationaux de données à caractère personnel notamment à des fins policières. Pour rétablir le lien de confiance avec l'usager tout en lui assurant un confort numérique dans sa relation avec l'État, il fallait faire preuve de pédagogie en créant un dispositif avec les mêmes fonctions et presque le même nom et le même design que Facebook Connect : FranceConnect. Ces similitudes ont sans doute permis de rendre ce moyen d'identification acceptable par les citoyens pour qu'il puisse s'imposer dans l'optique du 100% des services publics dématérialisés en 2022.

Depuis février, FranceConnect a obtenu par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) la qualification de sécurité « élevée » et est admis au titre de l'authentification électronique transfrontalière au sens du **règlement européen eIDAS du 23 juillet 2014**. La nouvelle plateforme, rebaptisée FranceConnect +, apparaît ainsi comme la clef de voûte du système d'information modulaire de l'État-plateforme dans laquelle l'identité numérique a vocation à

s'intégrer pour donner accès à des services nécessitant un niveau de sécurité élevé.

La CNIe va-t-elle servir, à court terme, de support à la création d'une véritable identité numérique souveraine ?

Aujourd'hui, ce nouveau document d'identité ne propose pas plus d'usages qu'un simple passeport. Or, l'identité numérique est un enjeu essentiel dans le développement des services en ligne qui repose sur la confiance réciproque dans l'identité des parties. Un très grand nombre d'acteurs économiques du secteur de la banque, des jeux en ligne, des assurances se montrent aussi intéressés par le développement d'une solution d'identité numérique régalienne. Il s'agit là également d'un enjeu sur le plan de la relance économique, puisque les entreprises françaises sont bien positionnées dans le secteur de la cybersécurité sur le marché de l'identité numérique qui devrait représenter 250 millions d'euros d'ici 2024 et plus d'un milliard d'euros d'ici 2029 (**rapport d'information de l'Assemblée nationale n° 3190 sur l'identité numérique**).

Or, contrairement à de nombreux pays européens (l'Estonie, la République Tchèque, l'Italie, l'Espagne, l'Allemagne, la Slovaquie, la Belgique, la Croatie, le Portugal, etc.), la nouvelle CNIe ne permet pas de s'authentifier dans des cas d'usage comme le vote en ligne, le dépôt de plainte, l'accès à son dossier médical ou pour des services en ligne de banques, de signature électronique des contrats, etc. La France accuse désormais un retard important vis-à-vis de ses partenaires européens qui ont presque tous mis en place une identité numérique comme la Belgique depuis 2003 avec désormais une application sur smartphone (« itsme »). En 2019, la France a testé une application de reconnaissance faciale ALICEM destinée à s'identifier pour se connecter *via* son smartphone aux services publics. En pratique, l'idée était de se passer d'une carte d'identité, d'un passeport ou d'une carte de séjour, et d'utiliser à la place une identité numérique. Les erreurs de jeunesse

d'ALICEM vont sans doute permettre de mieux cerner le futur dispositif d'identité numérique.

Si le lancement de la CNIe constitue le point de départ de la création d'une identité numérique, aucun calendrier n'a été annoncé concernant sa mise en œuvre. Or, selon la CNIL, « le déploiement de cette carte est l'occasion d'intégrer des outils supplémentaires permettant de garantir la meilleure protection de la vie privée possible dans le cadre de son usage comme support d'identité numérique » (par exemple, des dispositifs d'identification procédant à la divulgation sélective des informations présentes sur la carte comme en Allemagne). La Direction interministérielle du numérique (DINUM) œuvre pour que la CNIe permette à son possesseur de s'authentifier en ligne et cela en synergie avec le service d'identification FranceConnect. Le citoyen pourra toujours accéder aux sites des services en ligne avec ses comptes habituels car cette identité numérique ne sera pas obligatoire.