

# A S S E M B L É E   N A T I O N A L E

X V <sup>e</sup>   L É G I S L A T U R E

## Compte rendu

### Mission d'information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

- Audition commune, ouverte à la presse, de représentants :
  - du groupe Atos : Mme Coralie Héritier, responsable des identités numériques, dirigeante d'IDnomic ;
  - d'IN Groupe : MM. Romain Galesne-Fontaine, directeur des relations institutionnelles, et Yann Haguët, vice-président exécutif identité numérique, copilote du groupe de travail identité numérique au sein du comité stratégique de filière des industries de sécurité ..... 2

Mardi

6 avril 2021

Séance de 11 heures

Compte rendu n° 54

SESSION ORDINAIRE DE 2020-2021

**Présidence de  
M. Jean-Luc  
Warsmann,  
*président***



**Audition commune, ouverte à la presse, de représentants :**

**- du groupe Atos : Mme Coralie Héritier, responsable des identités numériques, dirigeante d'IDnomic ;**

**- d'IN Groupe : MM. Romain Galesne-Fontaine, directeur des relations institutionnelles, et Yann Haguët, vice-président exécutif identité numérique, copilote du groupe de travail identité numérique au sein du comité stratégique de filière des industries de sécurité**

*La séance est ouverte à 11 heures 10.*

*Présidence de M. Jean-Luc Warsmann, président.*

**M. le président Jean-Luc Warsmann.** Nous accueillons Mme Coralie Héritier, dirigeante d'IDnomic et responsable des identités numériques chez Atos, M. Yann Haguët, vice-président exécutif identité au sein d'IN Group, copilote du groupe de travail identité numérique au sein du comité stratégique de filière (CSF) des industries de sécurité, ainsi que M. Romain Galesne-Fontaine, directeur des relations institutionnelles d'IN Group.

Notre échange s'inscrit dans une réflexion sur l'identité numérique. La semaine dernière, nous avons auditionné les représentants de l'agence nationale des titres sécurisés (ANTS), du programme interministériel France Identité numérique, ainsi que le responsable d'une entreprise concernée par ce sujet.

Aujourd'hui, notre objectif consiste à mieux comprendre les choix technologiques qui s'opèrent à l'occasion du projet d'identité numérique régaliennne. Nous souhaitons également mieux cerner la façon dont les acteurs de ce projet interagissent au service de la meilleure performance possible et de la prise en compte des enjeux de souveraineté qui occupent nos travaux.

**M. Philippe Latombe, rapporteur.** J'évoquerai trois sujets sur lesquels nous aimerions vous entendre.

Le premier a trait aux enjeux de l'identité numérique et à la manière dont le déploiement de solutions publiques ou privées est susceptible de contribuer au renforcement de la souveraineté numérique de la France et de l'Europe. Quels choix technologiques ont été retenus et la position de l'Imprimerie nationale vis-à-vis de l'ANTS.

Pour parler sans détour, nous cherchons à savoir comment vous vous organisez pour définir ensemble des solutions techniques qui, dans le domaine de la sécurité, répondent à l'état de l'art. J'entends des solutions qui intègrent les dernières innovations. La question s'étend également à votre capacité à privilégier des solutions souveraines.

Le deuxième point intéresse le déploiement de la carte nationale d'identité électronique (CNIe), dont il était prévu qu'il s'effectue en lien avec une identité numérique. Vous ne l'ignorez nullement, cette perspective nourrit de fortes inquiétudes. Des parlementaires s'en sont récemment fait l'écho dans un courrier qu'ils ont adressé au Gouvernement.

Selon vous, comment s'explique le retard de déploiement que nous enregistrons, alors que la France s'avère déjà en décalage avec les autres pays européens ? Des marges de manœuvres, des moyens existent-ils afin d'accélérer le mouvement qui permettra d'apporter à nos concitoyens les nouvelles solutions disponibles ?

Enfin, nous reviendrons sur les usages de l'identité numérique. Je m'interroge, d'une part, sur les besoins et attentes des utilisateurs, d'autre part, sur les possibilités que ces solutions offrent ou offriront à terme.

J'apprécierais tout particulièrement de vous entendre sur le modèle économique de l'identité numérique. Il a fait l'objet de nombreux débats. À votre avis, quelle place les acteurs privés doivent-ils y prendre ? Comment convient-il de le financer ? En dernier lieu, de quelle manière rassurerons-nous les citoyens quant à la protection de leurs données personnelles, alors que la presse révèle régulièrement des affaires de fuites de ces données ?

**M. Romain Galesne-Fontaine, directeur des relations institutionnelles, IN Groupe.** Mon propos liminaire concernera IN Groupe. Structure publique, IN Groupe est l'imprimerie de l'État. Celui-ci en détient intégralement le capital. Spécialiste de l'identité et des services numériques sécurisés, IN Groupe opère au service de la mission régaliennne de réalisation des documents et des systèmes d'identité sécurisés. Il s'agit des passeports biométriques, des cartes nationales d'identité électroniques, des permis de conduire, des titres de séjour.

IN Groupe conçoit également les documents et systèmes qui permettent l'exercice d'un droit professionnel reconnu par l'État, telles que les cartes des agents publics, celles des conducteurs de poids lourds en France, ou la plateforme d'identité des professionnels de santé.

IN Groupe mène sa mission conformément au cadre légal applicable aux prérogatives de l'Imprimerie nationale exercées pour le compte de l'État.

Comme la plupart des membres de l'Union européenne, la France a choisi de s'appuyer, en matière d'identité, sur un opérateur industriel public capable d'intégrer de manière agnostique les meilleures technologies du marché. Ce choix permet à l'État de préserver sa souveraineté et son indépendance technologique, tout en garantissant la protection et la confidentialité de l'identité de ses ressortissants. De fait, l'Imprimerie nationale est amenée à connaître de l'identité de l'ensemble des Français.

Ses prérogatives trouvent leur contrepartie dans les engagements qu'elle prend vis-à-vis de l'État. Qu'il s'agisse des composants, des moyens de sécurité, des systèmes et des innovations, elle assure tout d'abord une veille technologique permanente dans le domaine de l'identité. Par cette action, elle apporte à l'État une maîtrise technologique à l'état de l'art. Elle lui garantit ensuite la sécurité de l'approvisionnement de ses titres d'identité, de leurs composants et des techniques qui concourent à leur fabrication. Enfin, dans sa démarche de sécurisation des titres, elle sélectionne les solutions techniques pour lesquelles elle sait compter sur au moins deux fournisseurs qualifiés ou qualifiables.

L'exigence en est devenue centrale depuis les crises de 2017 et de 2018. Les liquidations judiciaires inopinées et soudaines de fournisseurs risquent alors de compromettre la production des passeports français. Seules la mobilisation des réserves de sécurité de l'Imprimerie nationale et l'identification d'autres fournisseurs permirent de

maintenir la production. Ces situations ont conduit le ministère de l'intérieur, l'ANTS et l'Imprimerie nationale à entériner, en matière d'identité, une obligation de travailler simultanément avec plusieurs fournisseurs et de diversifier les sources d'approvisionnement.

Les fournisseurs retenus dans le respect des règles de la commande publique se soumettent de plus à une qualification industrielle stricte. Elle permet de vérifier leur capacité à fournir leur prestation à l'Imprimerie nationale pendant toute la durée de vie du titre. La qualification intègre ensemble des aspects techniques, économiques, de durabilité, de conformité aux normes et de sécurité d'approvisionnement.

À titre d'exemple, pour chaque approvisionnement stratégique, le choix des fournisseurs de l'Imprimerie nationale en vue de la production de la nouvelle CNIE a fait l'objet d'une sélection rigoureuse. De façon non exhaustive, je citerai le polycarbonate, les encres, le dispositif holographique, les composants électroniques, la plateforme de personnalisation ou les équipements de fabrication. Il est à noter que la plupart des entreprises partenaires du programme de CNIE sont françaises ou européennes.

L'enjeu consiste évidemment à assurer le déploiement généralisé de la CNIE, engagé le 15 mars 2021. La montée en puissance repose sur un outil industriel que nous avons dimensionné en conséquence. Nous aurons la capacité d'atteindre un volume de production et de personnalisation de 10 millions de CNIE par an. Pour la partie identité numérique de la carte, nous sommes aussi en mesure de poursuivre les travaux relatifs aux conditions de fourniture aux usagers d'un code confidentiel, ou numéro d'identification personnel (PIN, *personal identification number*).

Par ailleurs, pour le compte de l'agence du numérique en santé, nous développons le projet e-CPS. Il consiste en une version dématérialisée, sur *smartphone*, de la carte des professionnels de santé. Avec elle, nous évoquons une identité numérique que ces professionnels utilisent notamment pour se connecter au système informatique de l'assurance maladie.

IN Groupe mène aussi des activités à l'exportation. Elles contribuent à maintenir sa maîtrise de l'état de l'art. Le gouvernement monégasque nous a par exemple sélectionnés pour mettre en œuvre sa nouvelle plateforme d'identité légale, physique et numérique. IN Group lui fournira une carte d'identité électronique puis, à partir d'elle, une identité numérique dérivable sur *smartphone*, ainsi qu'une plateforme de services numériques.

Je compléterai mon propos en revenant sur une audition que votre mission d'information a conduite ce jeudi 1<sup>er</sup> avril 2021. Il me semble que l'une des personnes que vous avez entendues a fait montre d'approximation, voire vous a volontairement communiqué des données erronées.

En aucun cas la nouvelle CNIE n'équivaudra-t-elle à une simple copie du permis de conduire de 2013 ou du titre de séjour des étrangers.

Certes, comme ces titres, la CNIE doit respecter la réglementation européenne. Elle partage avec eux un cadre commun. Elle en partage encore quelques propriétés : le polycarbonate, le format d'une carte bancaire. Cependant, pour tout expert de l'identité, la ressemblance s'arrête là.

La CNIE inclut des sécurités de toute nouvelle génération. Elles n'avaient pas encore été employées. Son dispositif holographique utilise ainsi des nanomatériaux. Il autorise un contrôle variable optique. Inédit, le bord transparent de la carte prolonge le fonds sécurisé. Sa puce comprend un conteneur identité numérique développé avec l'industrie française. Un cachet électronique visible associe une signature numérique. La liste est longue des innovations visibles ou invisibles du nouveau titre. Des raisons évidentes de confidentialité m'interdisent de décrire les secondes.

La CNIE correspond à un titre dont les innovations côtoient des sécurités expérimentées et robustes. Les unes et les autres se conforment au cahier des charges de l'ANTS et des forces de police.

Une remarque avait porté sur un possible déséquilibre de la relation entre l'ANTS et l'Imprimerie nationale. Je rappelle qu'il s'agit d'une relation de confiance entre un donneur d'ordre public et un expert industriel public. L'ANTS, ainsi que les forces de police, établissent le cahier des charges sécuritaire d'un titre. Nous parlons alors de « cibles de sécurité ». En réponse, l'Imprimerie nationale propose une architecture qui combine un ensemble de sécurités physiques, électroniques et numériques. L'ANTS et les forces de l'ordre valident ensuite cette architecture : elles conservent donc le dernier mot sur la conception (*design*) et les aspects de sécurité du titre que l'Imprimerie nationale leur soumet.

Au cours de votre audition, des questions portaient sur la photographie du nouveau titre d'identité.

Avant toute chose, je préciserai qu'il ne s'agit pas d'une photographie en noir et blanc, mais d'une photographie en tons de gris. La directrice de l'ANTS a expliqué que la demande en provient des forces de l'ordre. Les raisons en tiennent au contrôle visuel, physique, du titre.

Ensuite, on a pu se demander si le procédé en était américain et ce qui avait justifié le choix de recourir à une technique étrangère.

Je déments ici un quelconque défaut de maîtrise technique : l'Imprimerie nationale peut parfaitement produire des titres en polycarbonate qui contiennent de la couleur. Elle le démontre à l'occasion de son partenariat avec le gouvernement monégasque. Il s'avère que 90 % de la centaine de pays qui, dans le monde, émettent des titres d'identité en polycarbonate, utilisent le système de gravure laser en tons de gris au cœur de la carte, choisi pour la CNIE française.

La technique en comprend deux blocs principaux : le matériau et les équipements de gravure laser. Une société européenne développe et fournit le premier. Les seconds se révèlent d'origine française. Une société située à Orléans, qui emploie 50 collaborateurs, produit et utilise ces équipements. Il se trouve qu'elle a fait l'objet d'un rachat, voici quelques années, par une entreprise américaine. La technologie que nous sollicitons n'en demeure pas moins française. Conclure que nous aurions opté pour un procédé américain au détriment de techniques d'une origine géographiquement plus proche de nous, paraît pour le moins contestable.

Enfin, s'agissant du cachet électronique visible de la CNIE, et ainsi que la directrice de l'ANTS l'a indiqué au cours de son audition, le projet n'a pas pu intégrer dans les premières phases de son développement la norme 105 car la publication de celle-ci ne remonte qu'au mois d'octobre 2020. En revanche, il reste loisible d'envisager une évolution conforme aux

spécifications de cette norme dans les prochaines phases du projet. La décision en reviendra à l'ANTS.

Nous nous confrontons souvent à des sollicitations de sociétés qui surenchérisent sur les aspects de sécurité en vue de promouvoir leurs solutions. Je rappelle qu'un titre d'identité se compose d'un ensemble d'éléments de sécurité qui répondent précisément aux cibles que le ministère de l'intérieur et l'ANTS ont déterminées. La surenchère que nous constatons ne nous apporte rien, à plus forte raison quand la technique dont elle vante le mérite n'a obtenu aucune reconnaissance en dix ans d'existence et qu'elle fait peser un risque certain en matière d'approvisionnement stratégique.

Je terminerai ma présentation en ramenant le débat sur un sujet central, celui de l'identité numérique. De véritables enjeux s'y décèlent sous l'angle de la souveraineté nationale.

En elle-même, l'identité ressortit à la souveraineté. Pour IN Groupe, elle constitue non un service, mais un droit fondamental. Il nous semblerait inconcevable que l'État ne prenne aucune part à la mise en place de l'identité numérique. Au contraire, par le moyen de la CNIe, l'État introduit un support qui autorise un large déploiement dans la population française, à l'attention de ceux qui le souhaitent, d'une ou plusieurs identités numériques sécurisées.

À notre niveau, nous nous réjouissons de contribuer à ce vaste projet. Nous saluons l'ambition et la qualité des travaux de son promoteur, le programme France Identité numérique.

Prête à fournir l'identité numérique des Français, l'Imprimerie nationale jouera son rôle au service de la stratégie de l'État, à l'instar d'autres acteurs publics ou parapublics, telle La Poste. Moyennant la délivrance du code confidentiel PIN de la CNIe, nous pouvons dès 2021 déployer la solution d'identité numérique que nous avons développée.

Ici, souveraineté nationale et souveraineté européenne se combinent. Par sa puissance normative, face à d'autres modèles qui émergent à travers le monde, l'Europe doit incarner une troisième voie dans la société numérique : celle de la protection des données personnelles et de l'identité. Elle se distinguera alors d'un modèle de monétisation de la donnée personnelle, ainsi que d'un autre modèle où données et identité numériques serviraient au contrôle social.

**Mme Coralie Héritier, dirigeante d'IDnomic, responsable des identités numériques du groupe Atos.** Je comprends que j'interviens devant vous principalement en ma qualité de copilote d'IN Groupe auprès du comité stratégique de filière (CSF) sur le projet identité numérique et en tant qu'experte de l'identité numérique.

Je vous présenterai le groupe Atos puis, en son sein, l'activité relative à l'identité numérique qui retient aujourd'hui notre attention.

Le groupe Atos est issu de la réunion de plusieurs acteurs du conseil et des services du numérique, ou technologie de l'information (*information technology*, IT) : Sligos et Sema Group, puis Siemens IT Solutions and Services et Bull. Son histoire a conféré au groupe Atos une dualité d'activités complémentaires, entre les services numériques et des produits intéressants des domaines comme la cybersécurité ou les supercalculateurs. S'ajoute une activité de recherche et d'innovation en matière d'informatique quantique.

D'une manière générale, le groupe Atos soutient le développement numérique de ses clients. À ce titre, il s'attache aux questions de cybersécurité. L'identité numérique figure au nombre de ces questions. Elle forme en effet l'un des piliers qui assurent la confiance indispensable au déploiement des activités numériques.

Anciennement Keynectis SA, spécialisée en cybersécurité, l'entreprise IDnomic a rejoint le groupe Atos en octobre 2019. À cette date, elle assurait déjà le copilotage du groupe de travail consacré au projet identité numérique du CSF des industries de sécurité.

IDnomic conçoit des certificats électroniques, selon une technologie d'infrastructure à gestion de clés. Celle-ci apporte des éléments de sécurité, comme le chiffrement de communications ou de fichiers, de l'authentification forte, la signature électronique. Nous l'avons tôt mise en service, en sous-traitance de l'Imprimerie nationale, désormais IN Groupe, et en partenariat avec l'ANTS. Son utilisation a d'abord concerné les passeports électroniques, devenus biométriques, français. Nous l'avons ensuite exportée. Elle a servi au déploiement des passeports d'environ trente autres pays.

Dans le processus d'émission des passeports biométriques, nous avons fourni avec cette technologie une chaîne de sécurité et de confiance.

**M. Philippe Latombe, rapporteur.** Sur l'identité numérique et, en particulier, la CNIe, pourquoi avons-nous pris autant de retard en France ? Pourquoi avons-nous dû, dans l'urgence, nous diriger vers une solution dont l'Union européenne nous avait d'assez longue date montré la voie ?

**Mme Coralie Héritier.** La réaction française n'est cependant pas si récente. Avec IN Groupe, nous appartenons aux acteurs qui nous trouvons au cœur de la question depuis des années. Nous avons œuvré dans différentes commissions, à des projets tels qu'IdéNum. Le Parlement s'est également saisi du sujet. Le frein qui y fut mis eut une origine essentiellement politique. Il ne m'appartient pas d'insister sur cet aspect. Sans doute, la société ni le monde politique français n'étaient-ils suffisamment prêts.

Désormais, la réponse que nous apportons se conforme parfaitement au Règlement européen. J'évoquais les passeports biométriques précisément parce que ce Règlement tend à généraliser les exigences qui, à l'instigation de l'organisation de l'aviation civile internationale (OACI, ICAO en anglais), prévalent en matière de transport aérien.

**M. Philippe Latombe, rapporteur.** S'agissant de la carte nationale d'identité, nous avons le sentiment que des pays européens ont été nettement en avance sur la France. Je pense en particulier au Portugal. Il semble qu'il en aille de même en matière d'identité numérique. La France paraît très en retard. Ce constat a incité, voici quelques jours, plusieurs de mes collègues parlementaires qui ont conduit la mission identité numérique à écrire au Premier ministre. Ils lui demandent d'intervenir pour hâter les réalisations françaises dans ce domaine.

La base réglementaire existe. Que se passe-t-il donc pour que nous accusions un tel retard ? La question reste ouverte.

**M. Yann Haguët, vice-président exécutif identité numérique d'IN Groupe, copilote du groupe de travail identité numérique au sein du comité stratégique de filière des industries de sécurité.** Je n'entrerai pas non plus dans des considérations d'ordre politique. Je puis néanmoins apporter certaines précisions. Par les retours d'expérience qui s'y

échangeant, le groupe de travail consacré aux enjeux d'identité numérique auprès du CSF des industries de sécurité offre un observatoire privilégié sur ces questions.

La genèse du programme s'avère plutôt ancienne. Elle remonte aux années 2000. Mme Coralie Héritier évoquait la multiplicité des commissions ou groupes de travail qui sont intervenus. Je puis citer le projet d'identité nationale électronique sécurisée (INES). La préoccupation a tôt existé. Les industriels se sont pareillement vite intéressés au sujet.

Le projet de protection des identités est apparu à partir de 2005. Il comportait deux volets. La France a d'abord choisi de concentrer ses efforts sur le problème du passeport, parce qu'il s'agit d'un document de voyage. Ils ont abouti en 2006 à la création du passeport électronique, en 2009 au passeport biométrique.

Au début des années 2010, la France s'est penchée sur la question de la CNIe. Par sa décision n° 2012-652 DC du 22 mars 2012, le Conseil constitutionnel a porté un coup d'arrêt à son élaboration. La décision de la Haute instance remettait en cause le principe de la mise en place d'une base centralisée des données biométriques de la population française, que la Commission nationale de l'informatique et des libertés (CNIL) jugeait par ailleurs irrecevable.

Il a fallu en conséquence retenir une approche non seulement différente, mais qui tînt compte de la pratique des autres États membres de l'Union européenne. Des événements sont ensuite intervenus.

Je pense d'abord à l'adoption le 23 juillet 2014 du Règlement européen n° 910/2014, relatif à l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (*Electronic Identification, Authentication and trust Services*, eIDAS). Il a significativement contribué à façonner la solution française de CNIe.

Il y a introduit la notion d'interopérabilité entre les identités numériques des différents pays, la nécessité d'utiliser un langage commun. Le Règlement eIDAS a eu le mérite de clairement caractériser les niveaux d'identité numérique : faible, substantiel ou élevé, et d'en définir les critères d'appréciation.

En 2014 toujours, l'apparition de FranceConnect a posé un autre jalon de la création d'une identité numérique à la française. FranceConnect correspond au souhait de l'État d'ouvrir à l'ensemble de ses ressortissants la possibilité de s'identifier sur un serveur unique, afin d'accéder à des services publics en ligne. Ce serveur fédère les identités numériques, il favorise lui aussi l'interopérabilité entre elles, standardise les critères d'identification des citoyens. À terme, conformément à la réglementation eIDAS, il jouera le rôle de nœud de connexion également pour des identités européennes qui, si elles y sont autorisées, pourront ainsi accéder à des services publics français.

Certes, la France a attendu le début de l'année 2019 avant d'entreprendre de définir précisément son modèle de CNIe et la manière dont elle y intégrerait la dimension d'identité numérique. La carte émise depuis le 15 mars 2021 applique les diverses spécifications, les choix et arbitrages qui sont intervenus depuis lors.

En obligeant les États membres à renforcer la fiabilité de leurs titres d'identité, l'Union européenne et sa réglementation ont joué un rôle de catalyseur. Le choix d'un mode

électronique garantit le respect de ces contraintes de sécurité. Il permet de plus de transformer la carte nationale d'identité en vecteur de diffusion de l'identité numérique.

**M. Romain Galesne-Fontaine.** Soyons clairs, la situation actuelle ne résulte nullement d'un défaut de maîtrise technique. Avec de nombreux acteurs français, l'Imprimerie nationale possède celle de l'identité numérique. Dès 2012, à l'occasion de l'adoption de la loi relative à la protection de l'identité, qui prévoyait la mise en place d'une CNIe, nous étions prêts. La censure du Conseil constitutionnel en a retardé la réalisation.

Toutefois, depuis 2019 et l'essor de FranceConnect, nous comprenons que le succès d'une identité numérique ne repose pas uniquement sur un support ou la fourniture d'une telle identité. Pour qu'elle atteigne ses buts, les exemples européens nous montrent que l'identité numérique suppose de fournir avec elle tout un ensemble, ou « écosystème », de services qui répondent à des usages. FranceConnect nous a justement permis de réfléchir plus avant à cet aspect décisif, que nous avons auparavant qu'insuffisamment considéré.

Désormais, notre démarche embrasse toutes les dimensions nécessaires à la réussite du projet. Ce projet d'identité et de services numériques sécurisés s'avère d'autant plus ambitieux qu'il concerne à terme une population de 67 millions de Français et un nombre proportionnellement élevé de connexions quotidiennes.

**Mme Coralie Héritier.** J'ajoute que dorénavant, à côté de la CNIe, l'identité, et même les identités numériques dérivées, gagnent en importance. Elles requièrent que nous nous projetions et poursuivions, notamment au sein du CSF, notre travail en commun avec les industriels de la sécurité.

Démocratisée, une identité numérique citoyenne et régaliennne doit permettre d'accéder à un autre niveau de services, pour des usages courants. Je pense notamment à la possibilité de l'employer depuis un *smartphone*. Je suis d'accord pour dire que son utilisation dépendra de l'étendue des services auxquels elle donnera accès. Il nous faut faire en sorte que l'identité numérique interagisse avec son environnement. Isolée de lui, elle ne sert à rien. Au contraire, l'interopérabilité et une large connectivité avec des services numériques lui conféreront toute sa valeur.

**M. Philippe Latombe, rapporteur.** Force est de constater que dans l'administration même, le réflexe perdure qui consiste à demander systématiquement des photocopies de la carte d'identité. À ce jour, il reste impossible d'engager une action en justice, d'immatriculer une société au greffe du tribunal de commerce, d'ouvrir un compte bancaire, voire simplement d'actualiser le dossier client qui s'y rapporte, enfin d'engager nombre de démarches, par exemple auprès de la caisse d'allocations familiales ou des organismes de sécurité sociale, sans produire une copie papier recto-verso de la carte nationale d'identité. Selon les cas de figure, il s'y ajoutera la demande d'une copie de la fiche d'imposition, ainsi que d'un justificatif de domicile, autrement dit une facture d'eau, de gaz ou d'électricité.

L'utilité de l'identité numérique ne laisse aucun doute. Prouver sa majorité sur Internet en donne un autre exemple.

**Mme Coralie Héritier.** Les progrès que la CNIe amène avec elle font présager une évolution rapide dans le sens que nous souhaitons. L'autorité nationale de la sécurité des systèmes d'information (ANSSI) vient de publier un référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID).

Lorsque nous parlons d'écosystème, nous nous interrogeons sur la manière d'adopter, grâce aux technologies disponibles, des solutions qui répondent aux usages que vous décrivez. Des prescriptions réglementaires, des référentiels adaptés nous le permettent dans des conditions de sécurité et de confiance qui garantissent l'intégrité ainsi que la fiabilité des données, et empêchent l'usurpation d'identité. Tel est bien l'un des objectifs que la CNIe poursuit.

**M. Romain Galesne-Fontaine.** Vos exemples, M. le rapporteur, ne manquent pas d'intérêt. Ils montrent combien la fourniture d'une identité numérique, outre qu'elle constitue un enjeu sur le plan de la sécurité, représente, ou peu s'en faut, un chantier de transformation culturelle. Elle emporte la modification d'un certain nombre de processus administratifs. Au préalable, il nous appartient de nous figurer comment ces services peuvent évoluer à l'aune du numérique.

Nous voyons qu'il s'agit à présent de travailler concomitamment à la conception d'une identité sécurisée et de penser la relation à l'utilisateur à l'ère du numérique. Ainsi dédoublé, l'effort requiert davantage de temps. Néanmoins, nous le pouvons considérer comme suffisamment avancé sur ces deux aspects pour affirmer que la CNIe, qui ouvre la possibilité de lui associer une identité numérique, offre désormais un outil efficace en vue d'une amélioration à brève échéance des services mis à la disposition des usagers.

**M. Philippe Latombe, rapporteur.** Bien que la CNIe soit prête, les usages ne suivront pas immédiatement son entrée en vigueur. Il suffit que nous songions à la carte vitale en matière de sécurité sociale. Le réflexe n'est manifestement pas encore celui d'une identité numérique à part entière. Dans les prochaines années, nous aurons toujours besoin d'un titre d'identité physique. La fracture numérique existe dans notre pays. Quand même elles en disposeront, des personnes n'utiliseront pas l'identité numérique et lui préféreront l'élément strictement physique de la carte pour justifier de leur identité.

La remarque me conduit à revenir, après vous M. Galesne-Fontaine, sur les auditions que nous avons tenues la semaine passée. Quoique vous affirmiez le contraire, il me paraît en ressortir que l'ANTS ne dispose plus, faute d'un effectif suffisant d'experts, de la maîtrise totale du projet. Vous semblez avoir pris une forme d'ascendant sur l'agence.

Je l'illustrerai par un exemple : actuellement, l'ANTS recherche un chef de projet CNIe.

C'est pourquoi je vous pose sans détour la question de savoir si la CNIe se situe réellement à l'état de l'art du point de vue de la sécurité. Nombreux sont ceux qui prétendent le contraire et estiment qu'elle accuse un retard dans ce domaine. À leur avis, d'autres pays en proposent le même format depuis plusieurs années ; certains ont indiqué depuis une grosse dizaine d'années.

Je prolongerai ma question par celle-ci : que coûte à l'État la production de la nouvelle CNIe ?

**M. Romain Galesne-Fontaine.** Sur votre première question, je rappellerai que l'Imprimerie nationale aurait été en mesure de produire une carte en polycarbonate dès 2012. Tel en était le projet. Des cartes de ce type existent donc depuis longtemps.

Pour autant, le fait que la nouvelle carte d'identité utilise le même matériau que des titres sortis dix ou quinze ans plus tôt revient-il à dire qu'elle présente des sécurités en tous points identiques aux leurs ? Je le répète : la réponse est négative. Je vous la donne en ma qualité d'expert industriel de l'identité. À l'Imprimerie nationale, nous travaillons pour plus d'une trentaine d'États à travers le monde, nous produisons régulièrement des titres d'identité modernes qui s'appuient sur les dernières innovations.

La CNIe française ne s'écarte pas de cette exigence. Elle comprend par exemple un dispositif holographique tout à fait original qui, composé de nanomatériaux, se distingue de l'habituel hologramme.

Au surplus, je n'affirme pas seul que la CNIe correspond à l'état de l'art en matière de sécurité. Pensez-vous que les forces de l'ordre françaises et l'ANTS, qui en ont supervisé le projet, en auraient validé la réalisation s'il en allait autrement et si elles avaient constaté que la carte ne répondait ni à leurs besoins ni à leurs prescriptions ? Je répète ici que l'Imprimerie nationale leur a soumis une architecture de sécurité destinée soit à prévenir les tentatives de fraude, soit à atteindre des objectifs de contrôle de sécurité sur le titre. La décision finale de valider cette architecture ne lui revenait pas.

**M. Philippe Latombe, rapporteur.** Sous l'angle des spécificités techniques, le format de CNIe, tel qu'il existe aujourd'hui, applique-t-il l'ensemble des préconisations que les spécialistes de la police aux frontières et de la gendarmerie nationale ont formulées ?

**M. Romain Galesne-Fontaine.** L'Imprimerie nationale s'est vu prescrire ce que nous appelons des cibles de sécurité. Elle devait y ajuster la nouvelle carte d'identité qu'elle mettait au point. Pour les atteindre, notre expertise tant nationale qu'internationale, notre veille technologique permanente, nous ont permis de combiner des éléments innovants de sécurité avec des solutions aussi robustes qu'éprouvées.

Nous ne saurions condamner des techniques qui ont apporté la preuve de leur efficacité en matière de sécurité au seul motif de leur ancienneté. À ce jour, nous n'avons connaissance d'aucun phénomène de fraude massive réussie sur nos titres français en polycarbonate. Jouant leur rôle, les sécurités en place ont permis de détecter immédiatement, à l'occasion d'un contrôle, les rares tentatives de fraude.

**Mme Coralie Héritier.** J'ajoute que l'ensemble des acteurs qui interviennent dans l'élaboration de la carte française ont exporté les technologies qu'ils mettent en œuvre. Ailleurs qu'en France, des titres d'identité les utilisent. Elles se conforment aux exigences en vigueur, notamment aux normes européennes. En aucune façon une moindre rigueur ne s'y attache dans le projet français.

**M. Romain Galesne-Fontaine.** Une partie des sécurités des titres que l'Imprimerie nationale produit, qu'il s'agisse des permis de conduire, des titres de séjour ou de la nouvelle carte d'identité, correspondent à des sécurités réglementaires. L'Union européenne les impose.

**M. Philippe Latombe, rapporteur.** Nous pourrions aussi nous interroger sur le point de savoir si la France trouve systématiquement un intérêt à reprendre à son compte les technologies que d'autres États utilisent.

Pour ce qui a trait au refus de recourir à la photographie couleur, je vous avoue n'avoir toujours pas saisi la raison qui le motive. J'entends l'explication relative au rachat d'une entreprise française par une entreprise américaine. Néanmoins, quand j'interroge des experts, y compris parmi les forces de l'ordre, on m'explique que la photographie en noir et blanc pose un problème opérationnel aux agents sur le terrain et que la couleur lui serait préférable.

Or, nous nous retrouvons avec une CNIe qui contient une photographie en noir et blanc. Pourtant, nous possédons la technique de la couleur, que nous ne manquons pas d'exporter. Le représentant d'IDEMIA, que nous auditionnions le 1<sup>er</sup> avril dernier, nous a indiqué que son entreprise l'employait. Pour leur part, grâce à leur partenariat avec leur entreprise nationale Veridos, les autorités allemandes, comme celles d'autres pays, utilisent une photographie en couleur sur leur CNIe.

Vous nous signaliez qu'en France, la demande d'une photographie en noir et blanc, ou en tons de gris, émanait de l'ANTS. Du moins ne vient-elle pas des forces de l'ordre.

Je réitère par ailleurs ma question sur le coût de revient, pour l'État, de la CNIe. À quel montant ce coût s'élève-t-il, à l'unité et tout compris ?

**M. Romain Galesne-Fontaine.** Nous pourrions partager avec vous, M. le rapporteur, les informations relatives au coût de la CNIe à la condition indispensable que l'ANTS y donne préalablement son accord exprès. Dans l'immédiat, au cours d'une audition publique, je ne puis vous les communiquer pour d'évidentes raisons de confidentialité.

**Mme Coralie Héritier.** Sans me prononcer quant à l'intérêt d'une photographie en couleur sur un titre d'identité, je signalerai que la nouvelle CNIe donne aux forces de police des possibilités de contrôle supplémentaires. C'est par exemple le cas du cachet électronique visible. Il facilitera leur travail sur le terrain.

**M. Yann Haguët.** La carte d'identité française fait appel à trois types de sécurité.

Nous venons de discuter en détail des sécurités physiques. Comme M. Romain Galesne-Fontaine l'a indiqué, elles correspondent à celles en vigueur dans la majorité des pays. Ici, notre devoir consiste à observer les pratiques qui prévalent, tout en nous assurant de la maturité des solutions que nous intégrons à notre projet.

À l'autre bout de la chaîne, la puce apporte elle-même un certain nombre de sécurités. Entre les deux extrémités, le cachet électronique visible (CEV) offre un premier niveau de lecture et de contrôle automatisé.

Au total, la duplication des éléments de sécurité confronte les éventuels fraudeurs à autant de barrages contre leurs intentions malveillantes.

Revenons à la question de la photographie en couleur. Dans l'élaboration de la CNIe, pour chacun de ses composants, pour tout élément de sécurité, l'un des points essentiels tenait à l'exigence de diversifier nos fournisseurs. Comme nous l'avons précédemment expliqué, nous devons nous assurer de la disponibilité d'au moins deux sources d'approvisionnement.

Or, les techniques de gravure de photographies en couleur disponibles sur le marché présentent la particularité d'être toutes différentes entre elles. De plus, aucune n'a complètement démontré sa capacité à traiter des volumes de l'ordre de ceux qui intéressent la

France. Jusqu'à présent, les projets qui y ont recouru trahissent ce que j'appellerai, courtoisement, une marge de progrès.

Sans remettre en cause vos témoignages de l'appréciation des forces de l'ordre, sachez que, parmi elles, des acteurs considèrent aussi que les dégradés de gris de la gravure laser donnent d'intéressants résultats en matière de contrôle et de détection des fraudes, là où les techniques en couleur peuvent pêcher en raison de caractéristiques différentes de sensibilité et de granularité de leur impression. Pour les forces de l'ordre, l'aspect essentiel du métier de contrôle consiste d'abord à se forger, à partir de l'image, une appréciation globale de points remarquables du visage, qu'elles comparent à la personne à qui elles font face. Elles n'analysent pas nécessairement le détail de la couleur. Assurément, il s'agit ici d'un débat d'experts et des avis divergents s'y feront toujours entendre.

En tout état de cause, la CNIe française ne saurait nourrir nul sentiment de malaise. Bien au contraire, il convient de reconnaître qu'elle intègre les meilleures techniques du moment, tant sous l'angle de sa sécurisation physique que du contenu de sa puce électronique. Peut-être y reviendrons-nous au cours de notre échange, c'est précisément dans cette puce que nous trouvons la base indispensable à la construction d'une identité numérique.

**M. Philippe Latombe, rapporteur.** Pour en terminer sur le problème de la couleur, je signale que les Allemands connaissent une problématique de volumes au moins comparables aux nôtres, voire supérieurs. Ils n'en utilisent pas moins une photographie en couleur.

À présent, évoquons en effet la puce de la CNIe, en particulier du point de vue de son évolution. La validité de la nouvelle carte court pendant dix ans. Une deuxième version en est-elle prévue ? Dans l'affirmative, à quel horizon ? À l'inverse, le même titre est-il appelé à se maintenir en l'état pendant la décennie qui s'ouvre ?

Au sujet de la norme 105, vous avez, M. Galesne-Fontaine, fait valoir un manque de recul pour une intégration immédiate à la CNIe. Cependant, des usages de l'identité numérique nécessiteront vraisemblablement que cette norme, ou un équivalent, soit tôt ou tard mise en application. Ce constat suppose une évolution du titre d'identité. Comment alors procéderons-nous ?

**M. Yann Haguët.** M. Galesne-Fontaine l'a souligné, la CNIe est d'ores et déjà configurée et prête pour l'identité numérique. Son système d'exploitation (*operating system*) et sa puce comprennent deux compartiments.

L'un, le compartiment ICAO, équivaut à celui d'un passeport. Il contient l'identité régaliennne. À la manière d'un passeport, il remplit la fonction que la réglementation européenne définit, celle qui permet à un citoyen de franchir les frontières internes à l'Europe. Son contrôle peut être automatisé.

L'autre, le compartiment d'identité numérique, respecte un standard français issu, entre 2019 et 2020, de l'intervention conjointe de l'ANTS, de France Identité numérique et des industriels, dont l'Imprimerie nationale, Thales et IDEMIA. Son déploiement ne suppose plus que son activation et, par un canal séparé et sécurisé, la transmission d'un code PIN à chaque citoyen français. Une fois activé, ce conteneur n'autorisera en effet son accès en lecture qu'à la condition que le possesseur du titre renseigne son code confidentiel.

Dès à présent, la CNIe contient donc un volet identité numérique. Il ne reste qu'à mettre en œuvre l'infrastructure d'un fournisseur d'identité. Ce fournisseur pourra être public ou, si la réglementation le prévoit, privé. Son rôle consistera à administrer l'identité numérique associée à la CNIe. Il interviendra par exemple si le titulaire de l'identité victime d'un vol souhaite révoquer sa carte.

Ainsi que le mentionnait Mme Coralie Héritier, il sera également possible d'étendre, ou « dériver », l'identité numérique associée à la CNIe à son utilisation à partir d'un *smartphone*. Une telle extension permettra deux types d'authentification pour des services publics ou privés.

La première, une identification de niveau élevé, au sens que lui donne la définition du Règlement européen eIDAS, se destine aux transactions les plus importantes, telles que l'ouverture d'un compte bancaire, la souscription à un emprunt bancaire ou la délivrance d'une procuration de vote. Elle impliquera que l'utilisateur approche la carte de son téléphone et saisisse son code confidentiel.

La seconde servira à des transactions d'un niveau de sécurité substantiel. On estime qu'elles recouvrent 80 ou 85 % des cas de figure. Elles ne nécessitent pas de recourir à la carte, l'identité numérique dérivée contenue dans le téléphone étant alors jugée suffisante.

Vis-à-vis d'un fournisseur d'identité, ces possibilités techniques impliquent que la réglementation lui permette d'utiliser le conteneur, ou compartiment, siège de l'identité numérique. Le fait qu'une décision rapide d'activation de ce conteneur puisse intervenir dès la délivrance de la CNIe requiert encore que son possesseur dispose de la faculté de s'enregistrer sans délai auprès d'un fournisseur d'identité. L'activation de l'identité numérique s'effectuera soit à partir d'un ordinateur personnel, après renseignement du code confidentiel, soit auprès d'un guichet public. Par l'intermédiaire de FranceConnect, elle rendra possible la connexion aux portails publics ou privés qui auront autorisé son utilisation.

Le fait que le service FranceConnect fonctionne déjà, qu'il ait récemment obtenu de l'ANSSI la reconnaissance d'un niveau élevé d'authentification au sens du Règlement eIDAS, qu'il définisse le format dit « pivot » des données à transmettre par chacun des fournisseurs d'identité, permettra à l'avenir un recours des plus étendus à l'identité numérique issue de la CNIe.

**M. Philippe Latombe, rapporteur.** Si je vous entends bien, la CNIe laissera à son détenteur le choix de son fournisseur d'identité, un fournisseur public ou privé ?

**M. Yann Haguët.** Techniquement, rien du moins ne s'y oppose. Il reviendra à la réglementation de préciser le dispositif, les conditions d'utilisation du conteneur et celles de l'agrément donné aux fournisseurs d'identité.

**M. Philippe Latombe, rapporteur.** La semaine dernière, Mme Valérie Péneau, inspectrice générale de l'administration, directrice du programme interministériel France Identité numérique, nous expliquait que, de son point de vue, aucun marché ne se dessinait pour une identité numérique privée. L'identité numérique lui paraissait ressortir exclusivement à la mission régaliennne de l'État.

Votre analyse contredit apparemment la sienne. Pensez-vous qu'il y ait place pour un marché privé de l'identité numérique ?

**M. Yann Haguet.** Je m'appuierai sur l'expérience d'IN Groupe à l'exportation. M. Romain Galesne-Fontaine le signalait, nous déployons l'identité numérique ailleurs qu'en France, notamment à Monaco. Notre pratique montre qu'une place existe tant pour un fournisseur d'identité régalién, autrement dit public, que pour des fournisseurs privés ou semi-privés.

Un fournisseur d'identité public garantit le niveau de sécurité le plus élevé. Il s'accorde avec le principe de gratuité qui, souvent, concerne la fourniture de l'identité ainsi que l'accès aux services publics.

Il n'en reste pas moins envisageable d'autoriser un système de fournisseurs privés ou semi-privés. Il existe dans certains pays. En France, La Poste, voire IN Groupe, pourraient revêtir cette qualité. Un tel système implique que les fournisseurs d'identité s'engagent à donner l'accès à des portails de services publics, au moins à un niveau de sécurité substantiel, par exemple, pour le paiement des impôts. Ils se rémunèrent alors auprès des fournisseurs de services en ligne qui recourent à l'identité numérique.

**M. Romain Galesne-Fontaine.** Pour compléter ce propos, j'estime qu'il serait opportun de reprendre les différentes études économiques qui ont concerné le sujet, à la lumière de la survenue de la crise sanitaire et des conséquences qu'elle entraîne. Sans doute ne mesurons-nous pas pleinement combien la situation que nous vivons depuis plus d'un an provoque une accélération de la mutation numérique de nos modes de vie, qu'il s'agisse des usages privés ou des pratiques professionnelles.

Nous pensions déjà nécessaire de fournir une identité numérique dans un cadre à la fois public et privé. Désormais, il nous apparaît que le bouleversement que nous connaissons rend d'autant plus attractif un marché pour des fournisseurs d'identité privés. La décision en revient à l'État. L'agrément qu'il donnera aux fournisseurs d'identité veillera à leur respect des règles de sécurité et de confidentialité des données personnelles.

Au sein de l'Imprimerie nationale, nous reconnaissons à ces données un caractère unique. Elles nous paraissent requérir l'emploi des plus hauts niveaux de protection. En dernière analyse, du strict respect de cette exigence dépend l'adhésion des usagers aux systèmes d'identité numérique. Les usagers doivent recevoir la double assurance que leur fournisseur d'identité n'utilisera pas leurs données personnelles à leur insu et qu'il se révélera en mesure de protéger ces données contre toute atteinte extérieure.

**M. Philippe Latombe, rapporteur.** La fourniture de l'identité numérique correspond-elle à un segment d'activité sur lequel IN Groupe entend se positionner ?

**M. Romain Galesne-Fontaine.** En effet, avec la perspective d'accélérer la mise en place de l'identité numérique en France, nous nourrissons l'ambition d'en devenir un fournisseur. Nous interviendrions en complément de solutions d'identité régaliennes. Les technologies dont nous disposons nous permettraient d'assurer, en application du Règlement eIDAS, le niveau substantiel de sécurité.

**M. Philippe Latombe, rapporteur.** Vos propres ressources internes vous suffiraient-elles ? Pourriez-vous vous passer de partenariats ?

**M. Romain Galesne-Fontaine.** Je vous le confirme. Nos moyens nous autorisent à prétendre à un statut de fournisseur agréé d'identité numérique, pour autant que l'État crée ce statut.

**Mme Coralie Héritier.** Comprenons que tous les acteurs auront une place à prendre. En tant que telle, l'identité citoyenne ne peut exister seule.

Sur un plan numérique, l'identité est susceptible de revêtir différentes formes. Il s'agira par exemple d'un certificat électronique. Cependant, dans les divers services et applications auxquels elle donnera accès, il lui faudra être associée à d'autres facteurs d'identification.

L'idée de multiplier ces facteurs gagne en importance. Le code confidentiel en est un. Il importera qu'ils se complètent entre eux, afin d'atteindre le plus haut niveau possible de confiance.

Ne concevons pas la CNIe comme le sésame unique qui répondrait à l'ensemble des besoins. Un véritable écosystème de l'identité numérique existe déjà. Il tend à s'étoffer, il se développe avec l'évolution des techniques. Pour leur part, les usages connaissent une croissance considérable. Ils requièrent l'emploi des facteurs multiples d'authentification que j'évoquais.

De ce point de vue, la gestion des identités numériques, celle de leur cycle de vie, s'avérera fondamentale. Une réglementation devra l'étayer. Le rôle d'en contrôler le respect incombera vraisemblablement à l'ANSSI.

**M. Philippe Latombe, rapporteur.** Nous accusons un tel retard sur le sujet de l'identité numérique qu'il est à craindre qu'il ouvre une porte, comme dans d'autres domaines avec les Google, Apple, Facebook, Amazon et Microsoft (GAFAM), à des entreprises privées qui imposent leurs propres standards. Non sans raison, des collègues parlementaires ont adressé un courrier au Premier ministre dans lequel ils mettent en exergue l'ampleur de notre retard. En comparaison d'autres États européens, celui-ci est indéniable.

**M. Yann Haguët.** Je souhaite apporter un complément de réponse sur la question de la maintenance du titre d'identité. Vous nous interrogez sur le devenir de la CNIe pendant les dix années de sa validité et sur ses éventuelles versions successives.

N'importe quel titre d'identité représente un état des techniques de sécurité disponibles à un instant précis. Il s'ensuit une forme de course-poursuite, aux échéances plus ou moins rapprochées dans le temps, avec les fraudeurs. L'apport de sécurités supplémentaires peut devenir nécessaire à tout moment.

Par le passé, avec les titres à sécurités purement physiques, la fréquence de nos interventions s'espaçait dans le temps. Dorénavant, l'emploi de l'électronique, de systèmes d'exploitation, d'algorithmes cryptographiques, conduit à la resserrer. En quelque sorte, le temps s'accélère.

Pour les cartes prochainement émises, IN Groupe a proposé à l'ANTS le recours à un gestionnaire du cycle de vie du titre et des versions de son système d'exploitation. Il lui reviendrait de procéder, en cas de besoin, à des opérations de maintenance de sécurité, de modifier ou d'activer des algorithmes de cryptographie, voire d'intégrer de nouvelles applications informatiques.

Un titre d'identité qui comprend une dimension électronique doit évoluer avec son environnement. Garantir que la CNIe assure sa fonction, y compris pour sa partie identité numérique, impose au minimum de respecter les contraintes du référentiel général de sécurité (RGS). Ces dernières prévoient le changement régulier des clés utilisées pour cryptographier les données et le processus qui permet d'y accéder.

Par ailleurs, en accord avec l'ANTS et sous sa direction, des phases de décision de nouvelles versions du titre interviendront. Elles correspondront à l'émergence de besoins ou usages, ainsi que vous le mentionniez M. le rapporteur, ou tiendront compte de celle d'autres règles ou contraintes européennes. La situation s'en est présentée avec l'actuel titre de séjour français. L'ancienneté de sa version dite V1 remonte à moins de dix ans. Voilà six mois, il a fallu redéfinir une nouvelle version, afin d'intégrer les évolutions que l'Union européenne imposait.

Un titre d'identité vit. Le principe de départ veut que son possesseur le détienne pendant dix années. Sauf cas exceptionnel, durant toute cette période, sa version initiale ni son apparence globale ne font l'objet d'une remise en cause radicale. En revanche, de réguliers changements de clés et, si nécessaire, des adaptations et mises à jour de sécurité en accompagnent l'existence.

Les versions des titres évoluent donc. Il est ainsi permis d'imaginer, d'ici à quelque temps, une version V2 de la CNIe.

**M. Philippe Latombe, rapporteur.** Quelle entité assurera-t-elle le suivi ? IN Groupe jouera-t-il ce rôle ?

**M. Yann Haguët.** Tout changement dans le système d'exploitation, toute introduction d'un élément de sécurité destiné à y combler une faille, suppose des échanges et l'activation de mécanismes dans un réseau plutôt fermé d'acteurs.

La décision d'opérer des changements relève du ressort de l'ANTS, en coordination avec l'ANSSI.

Selon les circonstances, nous pouvons envisager, soit une modification qui ne concerne que les futurs titres, soit à l'inverse une modification qui affecte l'ensemble de ceux déjà distribués, soit, dans les situations les plus graves, un remplacement pur et simple de la carte.

Certains cas de figure justifieront un retour de l'utilisateur devant les services de sa mairie. Moyennant des authentifications et des contrôles, des changements de clés mineurs pourront s'effectuer depuis un ordinateur personnel ou un *smartphone*.

**M. Philippe Latombe, rapporteur.** Soumettez-vous la CNIe à des tests de vulnérabilité, aussi bien physiquement qu'électroniquement, afin de la protéger contre les atteintes des faussaires ou des pirates informatiques ?

**M. Yann Haguët.** Nous réalisons évidemment de tels contrôles de sécurité. Chacun des industriels parties prenantes à la conception de la carte, en particulier de sa puce électronique et de son système d'exploitation, participe sous le contrôle de l'ANSSI et de laboratoires indépendants à un processus de qualification et de certification. Ce processus doit démontrer que la carte remplit les critères de sécurité attendus, que ses mécanismes de défense atteignent le niveau de complétude et de sécurité souhaités.

J'ajoute que nos fournisseurs ont l'obligation de répéter régulièrement leurs cycles de certification et de prouver que leurs solutions demeurent valides au cours du temps. À cette occasion, l'identification d'un risque peut conduire à l'ajout d'un correctif.

Le fait que le titre inclut de l'électronique et des systèmes d'exploitation emporte qu'un nombre accru de mécanismes entrent en ligne de compte dans sa maintenance.

**M. Philippe Latombe, rapporteur.** Je vous poserai une question en rapport avec la commande publique. Comment IN Groupe favorise-t-il l'émergence ou la consolidation d'acteurs, ainsi que leur excellence sur la scène internationale, sur les aspects de sécurité des titres d'identité ?

Certes, IN Groupe assure directement, en interne avec ses compétences, un certain nombre de réalisations, mais il en sous-traite également d'autres. Comment vous y prenez-vous ? Privilégiez-vous d'abord vos propres compétences avant que de vous adresser à l'extérieur ? Passez-vous systématiquement des appels d'offres ou procédez-vous de gré à gré ?

**M. Romain Galesne-Fontaine.** Je l'ai dit, le rôle de l'Imprimerie nationale est celui d'un intégrateur agnostique des meilleures technologies du marché. Même s'il possède certaines d'elles en propre, IN Groupe ne travaille pas isolément. Dans le cas de la CNIe, il compte plus d'une quinzaine de partenaires privés, dont le groupe Atos, associés à la fourniture des différents composants du titre.

Il nous tient à cœur d'animer ce que je qualifie d'écosystème. Chaque année, notamment pour l'élaboration des titres d'identité sécurisés, l'Imprimerie nationale recourt aux services de plus de 400 sociétés réparties sur l'ensemble du territoire français. Les retombées économiques en représentent plusieurs dizaines de millions d'euros.

Quant aux titres sécurisés, nous respectons systématiquement le cadre légal et réglementaire de la commande publique auquel nous sommes soumis. La sélection de l'intégralité des composants stratégiques de la CNIe n'a pas échappé au principe. Ici, la procédure de la commande publique nous permet d'appliquer scrupuleusement notre obligation de diversification de nos sources d'approvisionnement par le choix d'au moins deux fournisseurs pour chacun des composants. Nous garantissons ainsi à l'État sa capacité à délivrer sans interruption ses titres d'identité pendant toute la durée de leur validité.

**M. Philippe Latombe, rapporteur.** S'agissant de la CNIe, il nous intéresserait que vous nous précisiez les valeurs de la répartition entre ce qu'IN Groupe réalise directement et ce qu'il sous-traite par la commande publique.

Dans l'immédiat, je n'attends pas de réponse chiffrée, vous nous l'apporterez plus tard. Vous nous signaliez précédemment que, sur les aspects de coûts, il vous fallait obtenir l'accord préalable de l'ANTS. En revanche, peut-être pouvez-vous déjà nous communiquer un ordre d'idée de la répartition ?

**M. Romain Galesne-Fontaine.** Pour des raisons de sécurité, je ne puis non plus indiquer le nombre exact des composants stratégiques qui entrent dans la fabrication de la CNIe. Je vous disais qu'il avoisinait une quinzaine. L'Imprimerie nationale n'en fournit que deux. Vous obtenez là un aperçu assez clair du ratio qui vous intéresse.

**M. Philippe Latombe, rapporteur.** À ceci près que l'étendue des prestations respectives et de leurs montants, qu'en l'état nous ignorons, est susceptible de relativiser considérablement la pertinence d'une conclusion hâtive.

Sous l'angle de la souveraineté, prêtez-vous une attention particulière à la nationalité de vos fournisseurs potentiels ? Au contraire, ce critère n'entre-t-il pas en ligne de compte ?

**M. Romain Galesne-Fontaine.** L'ensemble de nos achats respectent les principes de la commande publique. Nous agissons dans la stricte limite que ces principes nous fixent.

Parmi les fournisseurs des composants de la CNIe, nombreux sont ceux d'origine française ou européenne.

**M. Philippe Latombe, rapporteur.** Voulez-vous aborder un sujet que nous n'aurions pas encore évoqué ?

**M. Yann Haguët.** Il convient de souligner combien la réussite du déploiement de l'identité numérique renvoie aux usages, à leurs approches, aux conditions de création d'un écosystème. Sans doute l'expérience de Mme Coralie Héritier au sein du groupe Atos et du CSF des industries de sécurité lui permet-elle de se forger une opinion sur la probabilité du succès de l'entreprise ?

**Mme Coralie Héritier.** Je vous avouerai ma perplexité quant à la raison pour laquelle la mission d'information m'a invitée à intervenir devant elle. Je note que la plupart des questions ont concerné l'Imprimerie nationale. J'aurais souhaité un débat à l'objet moins resserré. Cependant, je vous ai exprimé mon point de vue sur ce que l'identité numérique citoyenne devrait recouvrir.

Chez Atos, nous retenons une acception large des questions numériques ; nous considérons la transformation numérique en général. À notre sens, l'identité numérique en forme certes un pilier, mais non le seul. Il faut lui ajouter toutes les infrastructures, le *cloud* de confiance à qui il revient de supporter le volume des données, les outils, concevoir au surplus des socles mutualisés à destination de l'administration publique. À la vérité, bien des sujets nous permettraient d'étendre la discussion au-delà de la seule CNIe.

**M. Philippe Latombe, rapporteur.** La semaine dernière, lors de notre audition de Mme Valérie Péneau, nos questions relatives aux usages des identités numériques ont trouvé peu d'écho. En toute franchise, notre interlocutrice fut assez évasive. Il semblerait que nous ignorions encore ce que seront ces usages.

Pour l'heure, l'utilisation de l'identité reste plus physique que numérique. Sans doute appartient-il à cet égard à l'administration française de changer de paradigme et de mode de fonctionnement. L'identité s'inscrit au cœur de la transformation numérique de l'État. Nous nous en ouvrirons à Mme Amélie de Montchalin, ministre de la transformation et de la fonction publique.

Madame Coralie Héritier, vous semblez établir un lien entre *cloud* et identité numérique. Voici qui nous surprend. Pouvez-vous nous en préciser la nature ? Le premier conserverait-il les données de la seconde ?

**Mme Coralie Héritier.** Afin de traiter des volumes importants de données relatives à l'identité numérique, la chaîne de confiance utilise des technologies, notamment des

certificats électroniques. Privé, le *cloud* que j'évoque ne correspond pas à la définition que l'on donne ordinairement de ce terme. Pour ma part, j'entends par lui des infrastructures fiables, dont des opérateurs de services de confiance, dûment habilités, se chargent de la gestion. Elles permettent d'industrialiser tous les éléments de sécurité nécessaires à la création des identités numériques. En définitive, elles ne diffèrent pas significativement des techniques d'industrialisation du *cloud* au sens strict.

Pour une société comme Atos, partie au projet européen d'infrastructure de données GAIA-X, développer des capacités de calcul importantes, anticiper les évolutions post-quantiques à venir, lui sont indispensables pour se maintenir à l'état de l'art.

**M. Philippe Latombe, rapporteur.** Quel usage de l'identité numérique voyez-vous pour la France ? Quand y deviendra-t-elle la norme ?

**Mme Coralie Héritier.** Tout dépend d'abord du type d'identité dont nous parlons. De nombreuses identités numériques circulent déjà, qui ne sont pas d'un niveau de sécurité élevé et qui servent à accéder à un système d'information ou à une application en ligne. Certains en utilisent quotidiennement plusieurs. Elles sont entrées dans les mœurs.

À présent, il importe de mener une action de pédagogie sur l'usage d'une identité numérique d'un niveau de sécurité d'abord substantiel, puis élevé. Cette démarche favorisera la confiance des citoyens, elle-même primordiale pour le développement des usages numériques du quotidien.

L'évolution de l'identité numérique, sa démocratisation, reposent ensuite sur la facilitation de son usage.

L'authentification multifactorielle existe déjà. La directive européenne sur les services de paiement (DSP2) du 13 janvier 2018 l'a imposée pour toute transaction de plus de 30 euros. Chacun possède de même un code confidentiel attaché à sa carte bancaire. L'accès à des services en ligne sensibles ou à des données personnelles pourra encore tirer profit de l'authentification faciale, couplée à d'autres facteurs.

À mon sens, la banalisation de l'usage d'identités de niveaux de sécurité substantiel et élevé devrait devenir la règle assez rapidement.

**M. Romain Galesne-Fontaine.** Il nous faut réfléchir à des solutions d'identité qui soient inclusives. Personne ne saurait rester en marge de l'évolution en cours. Nous pensons que l'identité constitue un droit, non un service. L'universalité, l'effectivité, de ce droit supposent un langage compréhensible par tous, accessible y compris à ceux qui se tiennent fort éloignées de l'univers du numérique.

C'est pourquoi, nous nous attachons à mettre en place des systèmes qui s'appuient sur des procédures connues, tel que le code PIN. Nous travaillons de plus à l'élaboration de parcours d'usages aussi simples que possible, par exemple avec la dérivation de l'identité de la CNIe vers le téléphone portable.

Nous contenter de numériser des procédures fondées sur les documents du centre d'enregistrement et de révision des formulaires administratifs (Cerfa) équivaldrait à un échec. Aujourd'hui, l'occasion s'ouvre d'œuvrer à la simplification des parcours administratifs. La perspective en anime l'intention de nombreux experts engagés dans les programmes de transformation numérique de l'État.

**M. Philippe Latombe, rapporteur.** Je soulèverai une réserve. Nous ne contournerons pas l'obligation, sinon de conserver des guichets physiques, du moins de prévoir un substitut à la partie strictement numérique.

La situation actuelle en matière de délivrance et modification des cartes grises est éloquente. Pour la moindre demande, la numérisation intégrale de la procédure, l'impossibilité de se présenter devant les services de la préfecture, transforme un incident mineur en d'inextricables complications. Il en résulte une forte insatisfaction, notamment chez des personnes peu coutumières du numérique. En parallèle, nous assistons à l'émergence d'une économie de l'immatriculation des véhicules : partout en France, des officines apparaissent aux alentours des services préfectoraux, qui proposent aux administrés d'effectuer à leur place les démarches officielles d'immatriculation.

**M. Romain Galesne-Fontaine.** Je vous rejoins. Nous ne nous représentons pas un monde à 100 % numérique.

**M. Philippe Latombe, rapporteur.** Précisément, comment jugez-vous les expériences d'États qui ont opté pour un modèle intégralement ou presque intégralement numérique ? Il s'agit certes d'États plus petits que la France : l'Estonie, ou Israël qui a dans une large mesure numérisé les aspects d'identité et de santé. Néanmoins, gagnerions-nous à nous en inspirer ?

**M. Romain Galesne-Fontaine.** Les critères de réussite que nous avons identifiés dans ces pratiques de pays étrangers tiennent d'abord au rapprochement et à la coordination des divers acteurs et de leurs environnements spécifiques. En France, dans son essence même, le CSF des industries de sécurité participe d'une logique équivalente, avec l'objectif de fournir une identité, ou des identités, numériques sécurisées et de services.

En second lieu, un travail de pédagogie vis-à-vis de la population intervient. Il faut décrire les services que l'identité apporte. Il faut aussi expliquer que l'identité numérique a pour fonction de protéger, non de contrôler. Sans ce travail préalable, nous nous confronterons de nouveau en France aux débats que nous avons connus en 2012 sur les projets de CNIe et d'identité numérique, autour de la préservation des libertés fondamentales.

Non seulement nous devons insister sur ce que nos dispositifs respectent la législation et la réglementation en matière de données personnelles, mais sur ce qu'en outre ils contribuent à leur protection et offrent de nouveaux services.

Inclusion, pédagogie, travail avec un écosystème sur des services immédiatement utiles à la vie de nos concitoyens, nous engageons, me semble-t-il, dans la bonne direction.

**Mme Coralie Héritier.** Dans les pays qui ont choisi, ou peu s'en faut, le « tout numérique », la politique a pris appui sur quatre piliers : les infrastructures nationales, la diffusion des outils numériques dans tous les milieux et âges de la population, les financements dédiés à l'innovation et au développement des technologies tournées vers les usages, enfin l'identité numérique.

Nous pouvons nous en inspirer, même si chaque pays possède son histoire et son organisation administrative propres. En France, afin de réussir notre transformation numérique, je pense que nous aurions intérêt à promouvoir une forme de transversalité des actions que nos différents ministères mènent dans ce domaine. Nous poserions opportunément

des socles communs, en particulier sur les aspects de cybersécurité et d'identité numérique. Le partage d'applications informatiques, la coordination à tous les niveaux de l'État et de l'administration me paraissent essentiels. Pour leur part, les solutions techniques existent.

La coordination des services de l'État en matière numérique contribuerait de plus significativement à l'effort de pédagogie auprès du public.

Le CSF des industries de sécurité a exprimé son souhait de poursuivre sans relâche le dialogue entre les industriels et l'État. Dans l'élaboration des solutions numériques, particulièrement à l'occasion du plan de relance, nous apportons, en tant qu'industriels, notre contribution et notre vision. En retour, nous nous nourrissons des enjeux et ambitions de l'État.

**M. Yann Haguet.** Je partage cet avis sur l'importance de la coordination et de l'inclusion. J'ajouterais celle, clé à mes yeux, de la mixité entre les acteurs publics et privés.

À l'étranger, souvent les réussites sont apparues dès lors que l'État a favorisé l'implication du secteur privé et de la société civile dans la promotion de l'identité numérique, quand même celle-ci demeurerait attachée à une identité régalienne. Je pense par exemple à la Pologne. L'intervention du monde bancaire y a joué un rôle majeur. Pareillement, en Belgique, l'essor des usages de l'identité numérique a suivi l'initiative d'un consortium d'utilisateurs.

Le CSF des industries de sécurité a pour vocation d'encourager les échanges et la coordination entre les acteurs publics, les fournisseurs de services et les industriels. Cette coordination s'avère décisive quand, vous l'avez compris, la CNIE nous ouvre dès à présent le champ à une identité numérique.

**M. Philippe Latombe, rapporteur.** En somme, nous disposons avec elle du réceptacle de l'identité numérique.

*La séance est levée à 13 heures.*



### **Membres présents ou excusés**

#### **Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »**

Réunion du mardi 6 avril à onze heures dix

*Présents.* – MM. Philippe Latombe, Jean-Luc Warsmann

*Excusée.* – Mme Frédérique Dumas