ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

# Compte rendu

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



Jeudi
1er avril 2021
Séance de 9 heures 30

Compte rendu n° 51

SESSION ORDINAIRE DE **2020-2021**

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

ASSEMBLÉE NATIONALE

**Audition, ouverte à la presse, de MM. Pierre Lelièvre et Olivier Charlannes, vice-présidents de la société IDEMIA, et de M. Cosimo Prete, président fondateur de la société Crime Science Technology**

*La séance est ouverte à 9 heures 30.*

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

**M. le Président Jean-Luc Warsmann.** Avec MM. Olivier Charlannes, vice-président « Développement et marketing » de la société IDEMIA, Pierre Lelièvre, vice-président « Identité digitale » de cette même société et Cosimo Prete, président fondateur de la société Crime Science Technology, notre échange portera principalement sur l'identité numérique, qui s'entend comme la capacité à fournir aux citoyens et aux entreprises un moyen de s'authentifier avec un haut niveau de sécurité, lorsque ceux-ci accèdent à des services publics ou privés.

Nous nous intéressons aux enjeux de souveraineté technologique et de sécurité, afin de nous assurer que les solutions déployées sont les plus sûres et autonomes possible.

**M. Philippe Latombe, rapporteur.** Je souhaite d'abord que nous échangions sur les enjeux de l'identité numérique et sur la façon dont le déploiement de ces solutions, publiques ou privées, peut contribuer à renforcer la souveraineté numérique de la France et de l'Europe. À ce titre, j'aimerais vous entendre sur les choix faits, notamment dans le projet d'identité numérique régalienne, ainsi que sur le positionnement de notre pays par rapport à ses homologues européens. Le déploiement de ces identités numériques, qui devait intervenir à l'occasion du lancement de la carte nationale d'identité électronique (CNIe), suscite des inquiétudes sur lesquels vous nous donnerez votre avis.

J'aimerais ensuite que vous abordiez les conditions de réussite du déploiement de ces solutions auprès des citoyens et des professionnels, notamment sur les attentes et les besoins de ces utilisateurs, ainsi que sur les usages offerts par ces solutions. Nous pourrons ainsi prendre connaissance de l'état actuel du marché de l'identité numérique et échanger sur ses principales évolutions à venir. À cette occasion, nous évoquerons le modèle économique de l'identité numérique, qui a fait l'objet de nombreux débats. Concrètement, vous nous direz quelle doit être l'articulation entre l'action de la puissance publique et les solutions offertes par les acteurs privés dans ce domaine.

Je vous propose enfin de nous parler des enjeux de sécurité et de protection des données, qui préoccupent l'ensemble des utilisateurs de ce type de solutions. Vous nous indiquerez quelles sont leurs principales inquiétudes et comment les solutions d'identité numérique sont actuellement sécurisées.

**M. Pierre Lelièvre, vice-président « Identité digitale » de la société IDEMIA.** Je vous remercie de votre invitation. Pour IDEMIA, leader de la biométrie, il était important de pouvoir prendre part à ce débat.

De notre point de vue, l'identité numérique constitue la base de la souveraineté numérique de l'État, qui doit garantir une identité pour tous et assurer la sécurité de ses citoyens. Or, à l'heure actuelle, un citoyen sur six dans le monde ne dispose d'aucune identité. Ce point figure parmi les objectifs des Nations Unies pour 2030.

L'une des missions régaliennes de l'État est de garantir l'identité de ses citoyens, alors que notre économie se trouve actuellement en pleine transformation numérique, tirée par des nouveaux usages en ligne. Ces usages imposent aux États de nouveaux enjeux de lutte contre la fraude, notamment à l'identité connectée. Selon nous, l'introduction de la biométrie demeure l'un des moyens les plus efficaces pour y répondre, car celle-ci fait le lien entre le document physique et l'identité numérique, en réduisant les risques de fraude à l'identité.

IDEMIA maîtrise la sécurisation de l'identité, notamment grâce à la biométrie. Il s'agit d'un Groupe international issu du rapprochement de fleurons de l'industrie française. Nous sommes présents dans cent quatre-vingts pays et investissons plus de 200 millions d'euros par an en recherche et développement (R&D). Nous possédons également plus de mille cinq cents familles de brevets actifs. Nous sommes donc un pilier du numérique français, engagé auprès du Gouvernement pour favoriser la recherche et l'emploi, notamment en France. À titre personnel, je suis responsable du développement de l'identité numérique dans le monde, pour le secteur public.

En tant que leader de l'identité augmentée, notre objectif est de contribuer à une identité pour tous. Nous fournissons une réponse technologique de confiance, avec pour mission de créer un écosystème pour servir tous les usages. Ces usages peuvent être aussi bien publics (disposer d'un document d'identité, accéder à des services en ligne tels que l'éducation, la santé ou les aides sociales) que privés (souscrire à une ligne téléphonique, ouvrir un compte bancaire).

Depuis plus de quarante ans, le Groupe IDEMIA agit auprès des gouvernements, les accompagnant dans leur stratégie vis-à-vis de l'identité civile, à la fois par le biais de documents physiques sécurisés et de solutions s'appuyant pour partie sur la biométrie. Dans les années 1970, nous avons créé le premier capteur et le premier moteur d'analyse biométrique au monde, pour le compte du *Federal Bureau of Investigation (FBI).*

Depuis 2020, nous assistons l'agence européenne eu-LISA dans sa conception du système qui gérera les entrées et sorties du territoire européen. Il y a quelques jours seulement, nous avons été désignés, par le *National Institute of Standards and Technology (NIST),* numéro 1 dans le monde sur l'un de nos algorithmes d'analyse biométrique.

Il ne peut pas y avoir de souveraineté nationale sans identité numérique. En effet, la multiplication des services en ligne appelle au renforcement du niveau de sécurité. À ce propos, la crise sanitaire aura prouvé que certains actes essentiels au bon fonctionnement de notre système ont dû être stoppés ou reportés, en particulier les élections de mars 2020.

De façon plus générale, nous avons besoin d'accéder à une multitude de services de façon connectée. Or l'État demeure le seul acteur en mesure de vérifier l'identité de la personne se trouvant en face de nous lorsque nous sommes connectés. En ce qui concerne notre échange par Zoom de ce jour, je n'ai pas pu prouver mon identité. Il est donc urgent que nous puissions disposer d'une identité numérique.

Certains acteurs, notamment les géants du net, ont pu collecter pendant des années les données des citoyens français ou d'autres pays dans le monde, sans aucun encadrement. En Europe, le Règlement général sur la protection des données (RGPD) a corrigé une partie de ce déséquilibre, mais celui-ci existe toujours. À ce sujet, la souveraineté implique de pouvoir solliciter des acteurs locaux partageant les mêmes valeurs, respectant les mêmes lois et les mêmes codes éthiques. Pour autant, l'égalité de traitement n'est pas respectée.

La donnée est nécessaire au développement d'un logiciel d'analyse biométrique. Or pour l'heure, il nous faudrait des années pour accéder au même volume de données que certains de nos concurrents Nord-Américains ou Asiatiques, car la réglementation européenne actuelle ne nous permet pas de progresser à la même vitesse. Il est donc urgent de permettre à notre industrie de rester compétitive et d'avoir accès aux données de façon sécurisée, afin d'éviter les dérives observées dans d'autres régions.

Dans le secteur des télécommunications, certains acteurs européens comme Alcatel, qui ne disposaient pas du même appui gouvernemental que leurs homologues étrangers, ont vu leur position s'affaiblir. De la même manière que ce lien existe dans l'aéronautique, il devrait exister dans le domaine de l'identité, car il représente un enjeu majeur pour notre avenir.

Il est encore temps de renforcer le partenariat entre le public et le privé, pour compenser les déséquilibres. Notre intérêt n'est pas d'obtenir des subventions, mais de nous doter des moyens de rester dans la course. Pour y parvenir, IDEMIA souhaite la mise en place d'une réglementation permettant de protéger l'usager en respectant sa vie privée.

En parallèle, la compétitivité de notre industrie devra être soutenue. Nous pourrions par exemple nous inspirer de l'Allemagne, qui a transposé dans son droit interne la possibilité d'utiliser les données à des fins de R&D.

Nous devons protéger notre savoir et l'avance dont nous disposons encore. Plusieurs pistes existent, comme la création d'un label de fournisseur de confiance en matière d'identité numérique, dont la gestion pourrait, par exemple, être confiée à l'agence nationale de la sécurité des systèmes d'information (ANSSI). Il sera ensuite temps de définir ce que nous souhaitons mettre en place pour nos citoyens, en nous donnant les moyens de contrôler l'environnement mobile, de garder un droit de regard sur l'utilisation des données à des fins de recherche, ainsi que de disposer d'acteurs industriels supportant nos ambitions.

En France, un appel d'offres en cours devrait permettre de mettre en place la première étape de l'identité numérique. Si le retard pris s'explique en partie par la pandémie, tout retard supplémentaire n'enverrait pas un signal positif concernant notre capacité à nous doter d'un système d'identité numérique.

**M. Cosimo Prete, président de la société Crime Science Technology.** L'identité numérique et notre souveraineté sont des sujets qui me sont chers, car je suis un ancien expert de la police technique et scientifique.

Notre entreprise Crime Science Technology (CST) est spécialisée dans la fourniture de solutions de sécurité pour protéger les documents d'identité ou encore les billets de banque. Nous identifions également les personnes à partir de leurs empreintes digitales, grâce à des solutions déployées dans une vingtaine de pays dans le monde.

Chez CST, nous définissons la souveraineté numérique comme l'interaction harmonieuse entre l'État, les citoyens, les territoires et les acteurs économiques, dans l'intérêt du bien commun. Puisque la notion de frontière géographique n'a plus vraiment de sens dans le cadre du déploiement d'une solution d'identité numérique, il est important d'entretenir une relation de confiance entre les acteurs de l'industrie, les citoyens et l'État, afin de garantir l'identité de tous les individus.

S'il est désormais tout à fait possible de s'identifier à distance, rien ne dit en revanche que le support que vous tenez entre les mains est un document authentique. Il semble ainsi fondamental de combiner identité physique et numérique de manière harmonieuse, afin de pouvoir tirer le meilleur des deux mondes.

Les éléments déclinés à l'échelle européenne doivent pouvoir se retrouver au niveau national. Or nous sommes en droit de nous demander si le monopole régalien chargé de l'identité de confiance de tous les Français est en capacité de tirer le meilleur de ce que peut produire l'industrie française. Nous comptons des fleurons tels qu'IDEMIA ou Thales, plaçant la France dans le top 3 mondial des pays les mieux dotés en matière d'industrie de la sécurité. La question est de savoir si nous sommes en mesure de tirer le meilleur de tous les industriels et fournisseurs de solution, afin de garantir un niveau de sécurité maximal et une identité de confiance pour tous les Français.

Historiquement, la gestion des données n'a jamais été simple dans la culture française. Depuis l'après-guerre, une peur du fichage s'est même développée. L'enjeu est donc de regagner la confiance des citoyens, tant par une bonne gestion des données que par la manière dont celles-ci seront sécurisées sur les plans physique et digital. Chez CST, nous réfléchissons à cette relation de confiance, en prenant en compte les besoins opérationnels du terrain et les attentes des citoyens, tout en étudiant les meilleures façons de travailler avec les industriels pour déployer nos solutions.

L'organisation de l'aviation civile internationale (OACI) est une institution internationale chargée de formuler des recommandations de sécurité concernant les éléments électroniques, numériques et physiques des documents d'identité. C'est sur elle que s'appuie le Règlement européen pour concevoir nos titres français. Celle-ci produit également un état de l'art tous les trois ans. Je m'interroge toutefois sur la prise en considération de cet état de l'art dans notre identité numérique, tant sur sa composante physique que digitale.

En 2015, la Cour des comptes a affirmé qu'il était important de réfléchir à la façon de réguler le monopole d'État dans l'intérêt du bien commun. Or depuis la privatisation de l'Imprimerie nationale se pose la question de l'existence d'un conflit d'intérêts, car cette institution est devenue un centre de profits devant, dans le même temps, garantir la sécurité nationale. Il convient donc de s'assurer que nous disposons des outils de contrôle nécessaires pour tirer le meilleur de notre industrie.

**M. Philippe Latombe, rapporteur.** Vous avez indiqué que les géants du numérique avaient creusé leur avance, d'une part, en commençant à collecter les données plus tôt que nous, d'autre part, en bénéficiant d'un environnement juridique plus favorable à la poursuite de leur collecte. Quel type de données ont-ils collecté de manière massive ? Lesquelles vous seraient utiles en tant qu'industriels de la sécurité numérique ?

À ce jour, où en est la France par rapport à ses partenaires européens ? Existe-t-il des innovations apparues dans certains pays mais qui ne sont pas utilisées en France ? Connaissez-vous des pays situés hors de l'Europe présentant des niveaux de sécurisation de titres identiques ?

**M. Cosimo Prete.** Il y a environ trois ans, CST a été approché par la Bundesdruckerei (l'imprimerie nationale allemande), au sujet de notre solution de sécurisation *Optical variable material* (OVM). Cette technologie permet d'authentifier les documents en moins de trois secondes, aussi bien à l'œil nu qu'avec un simple appareillage. L'Allemagne a ainsi manifesté

son intérêt lors du salon mondial de la sécurité de Londres en 2018. Depuis cette date, nous travaillons en toute confidentialité avec l'imprimerie nationale allemande, pour réfléchir au déploiement de cette technologie dans ce pays.

L'Allemagne pratique une véritable veille technologie, en s'appuyant sur des budgets colossaux. Ainsi, en 2015, le budget R&D de l'imprimerie nationale allemande était huit fois supérieur à celui de son homologue français, s'appuyant sur une politique très forte en matière de propriété intellectuelle, ainsi que sur des partenariats tirant l'ensemble de l'écosystème vers le haut. Afin d'offrir le meilleur niveau de sécurité possible à ses documents, l'Allemagne ambitionne également d'aller chercher un certain nombre de solutions à l'extérieur. Ainsi, l'imprimerie nationale allemande construit et finance des programmes de R&D avec différents partenaires, notamment en collaboration avec les experts de la police allemande. Ces synergies ont permis à cette nation de mettre en place une identité électronique depuis une dizaine d'années. De son côté, la France reste l'un des derniers pays à déployer la sienne.

Le programme INES (identité nationale électronique sécurisée) a été lancé en 2005, posant les premiers jalons d'une CNIe. Du retard a ensuite été pris, probablement pour des raisons réglementaires quant à l'exploitation des données. Le projet de l'époque a alors été transféré sur le titre de séjour et sur le permis de conduire électroniques. Les technologies nécessaires étaient donc déjà disponibles, il y a une dizaine d'années. Avec les autres experts, nous ne comprenons pas comment autant de retard a alors pu être pris dans la conception de ce document, tant sur le plan physique que numérique. À l'inverse, les Allemands ont su mettre à profit ce qu'ils avaient accompli il y a une dizaine d'années, pour désormais évoluer.

Plusieurs centaines de milliers d'usurpations d'identité sont recensées chaque année en France. La fraude sociale se chiffre par exemple à 14 milliards d'euros pour l'État. Il est donc surprenant de constater que les moyens consacrés à la R&D demeurent limités, comparativement à ce que pratiquent nos voisins.

L'Allemagne scrute avec attention l'état de l'art triennal de l'OACI, dans lequel figure CST. À l'heure actuelle, une cinquantaine de technologies ont été identifiées à l'échelle mondiale, dont une quarantaine concerne la sécurité numérique et une dizaine la sécurité physique. Sur ces dernières, trois proviennent de chez CST. À ce stade, je m'interroge donc sur l'absence de ces solutions sur notre titre régalien, alors qu'elles profitent à des pays tels que l'Allemagne ou d'autres situés en Océanie. Il est en effet surprenant que la France ne soit pas capable de mettre en œuvre les meilleures solutions présentes sur son territoire.

La photo en noir et blanc figurant sur notre carte d'identité est fournie par une solution américaine, alors qu'IDEMIA ou Thales sont capables de produire une photo en couleur depuis plusieurs années. Une telle solution est déjà proposée dans des pays comme l'Estonie. Je m'interroge donc sur les choix technologiques ayant été faits, qui témoignent parfois d'un certain archaïsme. En effet, la moyenne d'âge des éléments de sécurité actuellement embarqués sur notre titre sécurisé dépasse la dizaine d'années, alors qu'il a paradoxalement été préconisé de limiter la durée de ce titre à dix ans, pour des raisons de sécurité.

Les innovations présentées par la presse n'en sont pas véritablement. Pour preuve, l'une des sécurités embarquées date d'il y a une trentaine d'années. Celle-ci a été préférée à une solution française figurant dans le dernier état de l'art. Cette tendance se vérifie également pour le cachet électronique visible (CEV), qui date d'il y a une dizaine d'années, alors qu'il serait possible de recourir à une norme universelle interopérable. Tous ces choix

suscitent des interrogations sur le pilotage des projets, ainsi que sur l'articulation entre l'agence nationale des titres sécurisés (ANTS), l'Imprimerie nationale et l'ensemble des fournisseurs français.

**M. Pierre Lelièvre.** Il faut établir une distinction entre le volet lié au document et le volet numérique de l'identité française. Ce dernier a été lancé en 1974, avec l'initiative SAFARI (système automatisé pour les fichiers administratifs et le répertoire des individus), qui s'est conclue par la création de la CNIL (commission nationale de l'informatique et des libertés). Nous avons donc pris le temps de bien étudier les différents modèles dont il était possible de s'inspirer. Un certain nombre d'expérimentations ont ainsi été réalisées en France, nous permettant de tirer de nombreux enseignements des initiatives passées. J'espère à présent que l'accélération dont nous avons besoin se produira dans les mois à venir, tant en matière de volume que de valeur apportée par l'identité numérique.

La qualité du résultat du développement d'algorithmes dépendra de la qualité de la donnée initialement injectée. Nous disposons encore d'une certaine avance en la matière mais sans accès à la donnée, cette avance finira par être remise en question. Or les GAFAM (Google, Apple, Facebook, Amazon et Microsoft) ont eu accès à un volume de photos sans précédent. L'enjeu est donc de pouvoir accéder à ces données, pour les transposer en informations biométriques et ainsi améliorer les performances de l'algorithme.

Dans le monde, il n'existe pas une façon unique de traiter un système d'identité numérique. En Europe, le modèle estonien sert de point de référence, avec une taille critique permettant de prendre des décisions plus facilement. Il a tout de même fallu près de vingt ans avant que ce système obtienne un taux de pénétration satisfaisant.

La vraie question pour la France est de savoir comment se donner les moyens d'une identité numérique accessible à tous. Pour y parvenir, le virage vers le « tout numérique » est souvent évoqué, mais celui-ci devra tout de même être accompagné, notamment de pédagogie. Des moyens humains seront nécessaires, afin de proposer des parcours alternatifs. Quoi qu'il en soit, l'utilisation d'un modèle complètement numérique ne nous semble pas réaliste et ne constituera pas un facteur clé pour créer la confiance entre les utilisateurs et la technologie.

L'Estonie se repose fortement sur son titre sécurisé équipé d'une puce permettant d'accéder à un panel de services en ligne. Dans ce pays, il est possible d'effectuer l'ensemble des opérations de la vie de tous les jours grâce à son identité numérique.

D'autres modèles étrangers s'appuient sur des infrastructures radicalement différentes. En effet, chaque pays où nous intervenons présente une législation et une population qui lui sont propres. En 2010 par exemple, l'Inde a démarré son virage vers l'identité numérique, en déployant le programme Aadhaar. L'État a alors demandé à ses citoyens de partager leurs informations biographiques et biométriques, dans un but de pratiquer la déduplication. Cette technique permet de valider qu'une même personne n'existe pas sous plusieurs noms différents. Plus de 90 % des 1,3 milliard d'Indiens ont été « embarqués » dans ce système. Équiper autant de personnes d'un titre sécurisé a toutefois représenté un coût très élevé.

En plus de disposer de documents sécurisés, certains gouvernements d'Amérique latine se sont par ailleurs dotés d'un système biométrique permettant aux différents acteurs des pays de vérifier l'identité des personnes.

De son côté, le modèle européen s'est tourné vers un titre sécurisé, pour des raisons historiques. Dans tous les cas, l'identité numérique implique de passer par plusieurs étapes. Il faut d'abord valider le document en lui-même, avant de s'assurer que sa date de péremption n'est pas dépassée. Seul le Gouvernement est en mesure d'effectuer ces opérations. Une fois le titre d'identité validé, ce même Gouvernement se charge d'y associer le porteur. Plusieurs technologies existent pour y parvenir. La biométrie est par exemple très largement déployée dans le monde, en raison de sa grande facilité d'utilisation.

**M. Philippe Latombe, rapporteur.** Le projet Aadhaar incluait effectivement les analyses biométriques des dix doigts et des deux iris. Le problème de la biométrie est que ces informations se retrouvent parfois à des endroits où elles ne devraient pas. Une partie des informations d'Aadhaar a ainsi été vendue par des pirates, pour se retrouver sur le dark web. Je me demande donc si la biométrie est suffisamment sécurisée ou si elle ne constitue pas au contraire une nouvelle mine d'or pour certains hackers, y compris au titre de l'Intelligence entre pays.

**M. Pierre Lelièvre.** Les logiciels IDEMIA sont utilisés en Inde mais le programme est ensuite géré en local. Le stockage et la protection des données n'a donc pas fait partie de notre champ d'action. Notre rôle est d'accompagner les gouvernements et de leur montrer l'état de l'art pour collecter ces données, les stocker et les gérer de façon sécurisée. Nous insistons par exemple sur la nécessité de séparer et de rendre anonymes un certain nombre d'informations.

**M. Philippe Latombe, rapporteur.** En France, au sujet de la sécurisation du titre ou de l'identité numérique associée, vos interlocuteurs sont-ils en capacité d'accepter ce que vous leur proposez ? À cet égard, le fait de recourir à une technologie américaine pour mettre une photo en noir et blanc sur un titre d'identité, alors même que des sociétés françaises comme Thales ou IDEMIA sont capables d'offrir de la couleur, pose question.

**M. Pierre Lelièvre.** Nous n'utilisons pas les photos sur la partie biométrique, car le procédé consiste, dans un premier temps, à transformer la matière brute. Ainsi, la photo est transformée en un *template* qui permettra d'en tirer une analyse biométrique, mais celui-ci n'est pas directement exploitable. Il sera alors stocké, *via* plusieurs niveaux de chiffrement. Les premières informations dont nous disposons sont donc stockées dans le coffre-fort de l'État.

L'identité est prouvée au moment de sortir son document. Il existe ainsi un décalage entre les usages demandés en ligne et les moyens dont nous disposons à l'heure actuelle pour nous authentifier.

Sur les documents physiques, nous investissons plus de 200 millions d'euros par an. Nous investissons également massivement dans des technologies liées à la photo, notamment en couleurs, permettant de valider que le document en présence a bien été émis par un gouvernement. Sur ce point, nous proposons de nombreuses technologies différentes aux gouvernements du monde.

**M. Philippe Latombe, rapporteur.** L'État pratique-t-il le *sourcing* ? Accepte-t-il de se pencher sur les nouvelles technologies ou préfère-t-il se réfugier dans une forme de conformisme ? Sur certaines solutions totalement numériques, les acheteurs publics n'ayant pas le temps de pratiquer le *sourcing*, ces derniers se contentent de passer des marchés publics qu'ils connaissent déjà. Cette tendance conduit à conserver des technologies anciennes et

généralement américaines, pour lesquelles l'ensemble des briques sont rassemblées en un même endroit. En toute logique, c'est l'ANTS qui devrait s'occuper de ces sujets. Quoi qu'il en soit, sommes-nous en capacité d'aller sourcer le meilleur de l'état de l'art, pour ensuite donner l'ordre à l'Imprimerie nationale de faire le nécessaire ?

**M. Pierre Lelièvre.** La sécurité s'apparente à une course contre des acteurs produisant des attaques et gérant de la fraude dans nos systèmes. Cette course ne connaît pas de fin et nous pousse en permanence à nous remettre en question et à développer des innovations. Par conséquent, ni la France, ni l'Estonie, ni aucun autre pays dans le monde ne se trouve à un niveau maximum de protection de ses documents d'identité, car il est toujours possible de faire mieux. Nous développons donc constamment des innovations, qui doivent ensuite accéder au terrain.

Au sujet de la CNIe, nous faisons partie des fournisseurs, notamment de la puce. Celle-ci permettra une évolution significative, en matière de niveau de sécurité, pour vérifier l'authenticité du titre. Cette puce respecte également tous les standards du marché.

**M. Olivier Charlannes, vice-président « Développement et marketing » de la société IDEMIA.** Il existe des technologies alternatives à celles ayant fait l'objet d'une décision du Groupe Imprimerie nationale. D'autres éléments de sécurité qui seront inscrits sur la CNIe ont en effet été sourcés sur le territoire français par le biais d'autres sociétés. Dans ce cadre, une évaluation est menée sur l'ensemble des fonctions de sécurité.

La sécurité d'un document physique dépend d'une combinaison de l'ensemble des fonctions de sécurité intégrées sur ce document. Or il nous est difficile d'affirmer qu'il aurait fallu ajouter telle fonction plutôt qu'une autre, car IDEMIA est actuellement partie prenante du projet de lancement de la nouvelle CNIe, en particulier au niveau de la puce et du logiciel embarqué. Ce dernier a été développé par nos équipes de R&D en France et a été certifié au plus haut niveau de sécurité par l'ANSSI.

**M. Cosimo Prete.** S'agissant de l'évaluation de la sécurité, les forces de l'ordre observent au quotidien les retours du terrain. Les agents disposent en moyenne de cinq secondes pour contrôler un document. Ils n'ont donc pas le temps d'examiner les changements de couleur, le nombre d'étoiles ou encore de tourner la pièce à quatre-vingt-dix degrés. Ils ont donc besoin de quelque chose d'intuitif, que tout le monde peut comprendre et mémoriser en moins de trois secondes. Les informations concernant l'évaluation de la fraude sont ensuite remontées au niveau de l'ANTS et de l'Imprimerie nationale, lorsque des réunions sont organisées, car la conduite du projet ne comporte aucun point d'étape.

La moyenne d'âge des éléments de sécurité est supérieure à une dizaine d'années. Hormis la puce, le package proposé s'avère ainsi plus ou moins équivalent à celui du permis de conduire ou du titre de séjour européen (TSE). L'année dernière, Europol a constaté que des falsifications de ces titres ont été retrouvées dans certaines officines de faussaires démantelées en France et en Europe. Or les spécialistes du ministère de l'Intérieur et les experts de l'Imprimerie nationale se sont aperçus que les mêmes techniques étaient employées pour le document d'identité nationale. Il semble donc surprenant que des combinaisons d'éléments de sécurité figurant sur des titres dits secondaires se retrouvent sur notre document régalien, qui se doit d'être le plus sécurisé de tous.

**M. Philippe Latombe, rapporteur.** Il me semblait que le ministère de l'Intérieur était le donneur d'ordre *via* l'ANTS et que l'Imprimerie nationale était l'exécutant. À cet égard, un

marché public doit avoir été lancé avec un cahier des charges. Comment se fait-il que le ministère de l'Intérieur n'ait pas déjà été au courant de ces éléments ?

Par ailleurs, il avait initialement été convenu que la CNIe et l'identité numérique seraient disponibles en même temps, alors que les deux ont finalement été décorrélées. L'État n'est-il donc pas en capacité de gérer ce type de sujets en mode projet ? Le retard de l'un a-t-il entraîné le retard de l'autre ?

**M. Cosimo Prete.** L'absence d'appel d'offres pour la partie relative à la conception physique du document constitue une véritable difficulté. Cette situation est liée au monopole régalien de l'État, qui exclut toute forme de compétitivité technologique et économique.

Une autre difficulté majeure concerne les effectifs de l'ANTS, qui ne comptent plus qu'un seul ingénieur spécialisé. L'agence cherche donc actuellement à recruter un chef de projet pour le programme CNIe, ce qui paraît inquiétant.

Il n'est pas possible d'être expert à la fois de la partie juridique, normative et industrielle. Or il me semble qu'une seule personne est pour l'instant en charge du sujet et le porte à bras-le-corps. Au final, une forme de déséquilibre se crée entre le donneur d'ordre et l'exécutant. Faute de pouvoir pleinement engager sa responsabilité, en raison d'un manque d'expertise, il me semble que le projet repose davantage sur l'exécutant.

Dans le même temps, l'avis des experts de la police et de la gendarmerie n'est plus écouté, car ces derniers s'autocensurent, faute de pouvoir exiger des technologies. Par conséquent, pour un élément de sécurité donné, l'ANTS affirmera que l'Imprimerie nationale ne lui a soumis aucune proposition, alors que l'Imprimerie nationale répondra que l'ANTS ne lui a pas demandé l'élément de sécurité en question. De fait, l'Imprimerie nationale finira par l'emporter, car c'est elle qui propose la combinaison figurant sur le document final.

Il n'existe pas de cahier des charges mais plutôt des cibles de sécurité posant une problématique opérationnelle de terrain, à laquelle une réponse tente d'être apportée sans y associer de nombre de sécurités. Tout le monde finit ainsi par se renvoyer la responsabilité, pour aboutir à une forme de raisonnement circulaire. À l'arrivée, une réponse est apportée à la cible de sécurité mais il n'est pas certain que celle-ci soit la meilleure possible.

Le Règlement de l'Union européenne formule des demandes très précises. Par exemple, pour une encre optiquement variable, différentes solutions existent sur le marché. Il est alors très simple de comparer les éléments de sécurité, au moins en ce qui concerne la partie physique. Ces éléments présentent trois niveaux de contrôle : à l'œil nu, avec un petit appareillage, en laboratoire. Un quatrième niveau sera bientôt ajouté, avec le téléphone portable. Lorsqu'un élément de sécurité retenu ne peut être vérifié que sur un seul niveau de contrôle alors qu'une autre technologie répondant à la même fonctionnalité peut se vérifier sur quatre niveaux de contrôle, je m'interroge sur la politique mise en œuvre. Il semble en effet que la politique du « moins-disant » soit privilégiée, par méconnaissance des éléments de sécurité et des technologies déployées sur le terrain.

En 2018, l'Imprimerie nationale a pris l'initiative, avec l'ANTS, de proposer notre technologie à la Commission européenne, pour sécuriser le TSE. La technologie a alors été éprouvée en profondeur par l'Imprimerie nationale. Nous avons ensuite été « retoqués », au motif que l'ANTS et l'Imprimerie nationale considéraient que notre technologie ne répondait pas à la norme. Trois ans plus tard, nous avons pourtant appris que la norme avait mal été

interprétée. Ironiquement, notre technologie en question est désormais classée dans le top 50 de cette norme.

**M. Pierre Lelièvre.** Je suis d'accord avec M. Cosimo Prete concernant l'importance de disposer de moyens pour contrôler l'identité sur le terrain.

Par ailleurs, le contexte actuel diffère radicalement de celui de 2019. Nous sommes ainsi contraints de nous connecter en ligne pour échanger, opérer ou effectuer des transactions. Aussi critique que soit la vérification des titres physiques, nous nous trouvons désormais en plein virage numérique. Cette tendance existait déjà depuis plusieurs années, mais connaît actuellement une forte accélération à cause de la crise sanitaire. Or, personne n'avait anticipé le niveau des attentes auxquelles nous sommes confrontés.

S'agissant de notre souveraineté numérique, nous faisons face à un déséquilibre, car nous nous trouvons face à des acteurs en position dominante maîtrisant l'environnement mobile. Le smartphone est désormais devenu totalement incontournable, dans le domaine privé comme dans le public. À l'heure actuelle, ces téléphones sont maîtrisés par deux acteurs décidant de ce qu'il est possible ou non de réaliser avec eux. Ainsi, certains choix commencent déjà à se fermer pour nous. Si nous ne prêtons pas la plus grande attention à la façon dont nous souhaitons nous positionner, en tant que nation ou en tant qu'Europe, face à ces acteurs gérant une partie de notre écosystème, nous finirons par rater le virage et il sera presque impossible de le rattraper.

Il convient donc de nous interroger sur notre façon d'utiliser les téléphones et sur les informations qui y seront disponibles. Dans le cas contraire, nous serons amenés à charger des informations liées à notre identité pivot sans savoir où celles-ci se retrouveront. Nous pourrions par exemple exiger de la part de ces acteurs un certain niveau de sécurité concernant la zone de stockage et la zone d'exécution. Il sera donc nécessaire de décomposer les étapes et les informations que nous avons besoin de partager, ainsi que de nous demander comment elles seront utilisées. Pour rappel, lors de la parution du RGPD, ces acteurs ont tenté de lutter contre les contraintes que celui-ci impliquait.

Nous nous trouvons à un point critique où un système d'identité numérique est en passe d'être lancé à l'échelle de la nation. Cette identité numérique reposera sur un certain nombre d'infrastructures. Les fournisseurs de service tels que les collectivités locales, les banques ou les opérateurs auront besoin d'accéder à l'information gouvernementale, car c'est bien l'État qui est en mesure de confirmer l'identité d'une personne. Cette information devra de toute façon être partagée sur certains supports, qu'il s'agisse d'ordinateurs ou de téléphones portables.

Nous avons donc besoin d'exprimer nos exigences et d'établir une certaine normalisation. Un premier niveau a été mis en place en ce qui concerne les données avec le RGPD. Un deuxième l'a également été avec le Règlement *eIDAS (Electronic Identification Authentication and trust Services)*, qui a permis d'atteindre un premier objectif d'harmonisation au sein de l'Europe. Nous devons désormais nous montrer plus spécifiques concernant nos attentes vis-à-vis des parties prenantes. Sur ce point, impliquer les GAFAM me paraît être une bonne façon de répondre à l'accélération face à laquelle nous nous trouvons.

**M. Philippe Latombe, rapporteur.** L'année dernière, les députés ont adopté une loi interdisant la simple déclaration de majorité sur Internet pour la visite de sites

pornographiques. Le conseil supérieur de l'audiovisuel (CSA) est en train de mettre cette loi en pratique, en demandant à ces sites de vérifier que les personnes souhaitant y accéder sont bien majeures. Comment y parvenir, alors que l'identité numérique n'est pas encore disponible ? Des pistes existaient autour du micro-paiement bancaire mais elles ont été rejetées par le CSA, car certaines cartes bancaires peuvent être délivrées avant l'âge de 18 ans. FranceConnect représente une autre option. Un système de capture d'écran pourrait également être envisagé, la personne montrant sa carte d'identité pour accéder au site.

Au final, nous ne sommes pas en capacité de mettre en œuvre la loi adoptée. Ce retard sur l'identité numérique n'est-il pas le signe que le sujet a été pris à l'envers ?

**M. Pierre Lelièvre.** Nous avons participé à un certain nombre de groupes de réflexion autour de la question des usages, animés par le ministère. Cette question se pose dans de nombreux pays, en lien avec le contenu de certains sites ou à la consommation de certains produits, pour lesquels il est nécessaire de prouver son identité ou son âge. La question est donc de savoir comment partager certaines informations sans forcément transmettre l'intégralité du contenu figurant sur nos documents d'identité.

Un moyen de pallier la difficulté est de considérer l'identité comme un service pouvant être offert par l'État à sa population. L'idée est de percevoir l'identité comme un besoin fondamental, en particulier l'identité numérique. Nous pourrions alors disposer d'un service de l'État auquel il serait possible de se connecter pour accéder à certaines d'informations pertinentes aux cas d'usage. Ainsi, dans le cas où l'âge d'une personne devait être vérifié, seule cette information serait disponible. Or il existe déjà des solutions permettant de ne contrôler qu'une partie des attributs définissant notre personne. À titre personnel, je ne souhaite pas partager mon adresse avec n'importe quel fournisseur de service ou acteur.

Quoi qu'il en soit, la technologie existe déjà et il nous reste désormais à définir la façon dont nous souhaitons la mettre en œuvre pour répondre aux différents cas d'usage.

**M. Philippe Latombe, rapporteur.** L'État dispose-t-il des talents nécessaires pour mener à bien ce projet ? J'ai cru comprendre que l'ANTS manquait d'experts.

**M. Pierre Lelièvre.** La France possède un vivier d'universités extrêmement pertinent. De notre côté en tout cas, nous ne rencontrons aucune difficulté pour recruter, tant pour les profils ingénieurs que commerciaux.

**M. Philippe Latombe, rapporteur.** L'État a-t-il la capacité de trouver des personnes à la fois intégrées en son sein et ouvertes sur le plan technologique, afin de pratiquer le mode projet ?

**M. Pierre Lelièvre.** Nous menons de nombreux projets avec le Gouvernement ainsi qu'avec l'Europe, sans pour autant rencontrer de problèmes de gestion. Dans ce cadre, nous émettons des recommandations, mais toutes ne sont pas entendues. Je suis en tout cas satisfait de nos échanges avec l'ANTS ou avec les forces de l'ordre.

L'État n'est pas seulement accompagné par des acteurs tels qu'IDEMIA ou des start-up, mais également par certains grands intégrateurs. Par exemple, l'appel d'offres sur l'identité numérique lancé en fin d'année sollicite l'aide de ces intégrateurs. Ainsi, le Gouvernement français semble bien conseillé.

**M. Philippe Latombe, rapporteur.** J'évoquais le mode projet car d'autres auditions ont mis en évidence que certains ministères n'étaient pas en capacité de gérer par projet.

**M. Pierre Lelièvre.** S'agissant de l'identité numérique, nous considérons que les moyens mis en œuvre sont insuffisants par rapport aux attentes et aux enjeux.

**M. Philippe Latombe, rapporteur.** Selon vous, les montants de l'appel d'offres semblent trop restreints ?

**M. Pierre Lelièvre.** Oui, très clairement. Je pense que nous ne sommes pas parvenus à nous maintenir dans les objectifs qui nous avaient été fixés. D'un point de vue technologique, cet appel d'offres répond vraiment à la situation actuelle, en prenant en compte différents types de documents à valider. Il permet également de se projeter vers l'avenir, avec l'utilisation de la biométrie.

**M. Philippe Latombe, rapporteur.** S'agit-il d'un appel d'offres alloti ou général ?

**M. Pierre Lelièvre.** L'appel d'offres est alloti, comme c'est souvent le cas à l'heure actuelle. Pour y répondre, un cahier des charges très précis a été formulé et a évolué en suivant certaines recommandations, notamment en provenance de l'ANSSI. Nous avons alors été amenés à travailler en consortium avec d'autres entreprises, chacune devant y trouver sa place. Nous n'avons toutefois pas été en mesure de totalement répondre aux conditions financières demandées, alors que notre réponse était cohérente sur le plan technique.

**M. Philippe Latombe, rapporteur.** Aucun appel d'offres n'a été lancé sur la partie relative au titre physique ?

**M. Cosimo Prete.** À notre connaissance, les éléments de sécurité physique de la carte n'ont fait l'objet d'aucun appel d'offres.

Je suis en grande partie d'accord avec les propos tenus par M. Philippe Lelièvre. Un élément m'interpelle cependant au sujet de l'authentification à distance. À ce propos, le CEV vient d'être présenté par l'ANTS, alors qu'un tel dispositif était encore inimaginable il y a deux ans. Les mouvements associatifs ont en effet dû batailler pour faire intégrer le CEV sur la carte. Le contraste semble ainsi saisissant avec les annonces du Président de la République. Si les associations n'avaient pas bataillé à travers des collectifs, notre CNI ne comporterait pas de CEV.

Le CEV ayant été adopté sur notre CNI en est à sa version 101 et non 105. Par conséquent, chaque fois qu'un nouveau cas d'usage n'ayant pas été prévu par le CEV actuel se présentera, il sera nécessaire de réactualiser l'ensemble du système. À l'inverse, la version 105 du CEV a été validée selon la dernière norme AFNOR pour être universelle et interopérable, avec une mise à jour des différentes fonctionnalités. Nous nous fixons ainsi nos propres limites, en adoptant la version 101 et non 105 du CEV, alors que cette dernière pourrait être lue hors de France.

Par effet ricochet, cette décision plombera d'autres projets comme le pass sanitaire (qui consistait à déployer une solution française à l'échelle européenne), à cause de l'absence d'un référencement national stratégique. Cette situation semble vraiment surprenante.

**M. Philippe Latombe, rapporteur.** Vous voulez dire que l'avenir n'a pas assez été anticipé ?

**M. Cosimo Prete.** Assurément.

Je ne suis pas favorable au « tout digital » ni au « tout physique ». Il faut plutôt combiner le meilleur des deux mondes de manière harmonieuse. À ce sujet, l'ANSSI a lancé en mars le référentiel d'exigences applicables aux prestations de vérification d'identité à distance (PVID). Si certains fournisseurs de solutions devront travailler à l'authentification à distance de ce document, il est aberrant de penser que toutes les données pourront être contenues dans un téléphone portable ou dans une carte. Il existe en revanche des technologies permettant de déterminer que le CEV placé sur le document et le document en lui-même sont tous les deux authentiques. Il ne faut donc pas chercher à opposer les deux mondes.

En l'éclairant à l'aide d'un téléphone portable, il est possible de faire changer la couleur du CEV et ainsi de prouver à la caméra l'authenticité du support et du CEV. Cette méthode sera déployée chez nos voisins alors qu'il s'agit d'une solution française. Nous ne sommes donc pas capables de préparer l'avenir. Des impératifs nous sont indiqués mais nous ne parvenons pas à nous donner les moyens intellectuels, économiques et industriels pour aller plus loin.

L'enjeu est de déterminer la part de mixité technologique entre les grands fournisseurs de solutions et le monopole de l'État pour préparer l'avenir ensemble. Nous rencontrons des difficultés sur ce point, notamment car les ressources dont nous disposons en matière de gestion de projet ne sont pas à la hauteur de nos ambitions.

**M. Philippe Latombe, rapporteur.** Notre identité numérique sera disponible bien plus tard que ce qui était initialement prévu. Combien de temps faudra-t-il attendre avant que celle-ci ne soit lancée ?

**M. Pierre Lelièvre.** Différentes étapes devront être franchies, mais il faudra un peu plus d'un an pour mettre en place la première brique de ce système d'identité numérique. Une partie est déjà disponible chez FranceConnect, qui doit généraliser certains éléments tels que l'accès à DOCVERIF. Ce système permet de valider un certain nombre d'informations auprès de l'État, par exemple pour vérifier qu'un document existe bel et bien ou qu'il est toujours en cours de validité. À l'heure actuelle, ces informations ne sont pas encore totalement généralisées dans le modèle.

Le seul fait de disposer d'une puce dans les documents permettra de débloquer un certain nombre d'usages en ligne, car ces puces demeurent des éléments extrêmement sécurisés. Elles sont par exemple utilisées dans les passeports pour passer les frontières. Elles permettent également de disposer d'une authentification de niveau élevé auprès des différents fournisseurs de services. À ce sujet, le Règlement européen considère la puce comme l'élément ultime qui permettra de procéder à l'authentification d'un document puis à l'identification d'une personne. Ce dispositif vérifiera notamment que la photo présente à l'intérieur de la puce correspond réellement à la personne en question. Plusieurs méthodes permettront d'y parvenir. L'ANSSI envisage de placer un humain de l'autre côté de la vidéo, mais il est également possible d'utiliser un système automatique. Quoi qu'il en soit, les deux approches devront être complémentaires.

**M. Philippe Latombe, rapporteur.** Le temps que l'identité numérique, telle qu'elle est prévue dans l'appel d'offres, soit mise en place, de nouveaux usages non prévus risquent-

ils d'émerger d'ici douze à vingt-quatre mois, générant ainsi un blocage à l'arrivée ? Cette éventualité a-t-elle été intégrée dans le process ?

**M. Pierre Lelièvre.** Des nouveaux usages émergent en permanence. En Estonie par exemple, il est désormais possible de voter avec son document d'identité.

**M. Philippe Latombe, rapporteur.** Le vote figure parmi les grands sujets que nous avons évoqués hier. Le conseil scientifique a en effet affirmé que si nous avions pu vérifier l'identité numérique des citoyens, il aurait alors été possible d'organiser des élections municipales et régionales dans des conditions sanitaires convenables. La question est donc de savoir si nous disposerons d'une interopérabilité complète pour assurer ces nouveaux usages, dont l'émergence n'est pas forcément encore connue.

**M. Pierre Lelièvre.** Il est nécessaire de protéger la santé de nos concitoyens, en leur offrant la capacité de voter en ligne. Dans le même temps, nous avons besoin de protéger notre République, en nous assurant que les élections se déroulent dans un certain cadre. À l'heure actuelle, je ne pense pas que nous soyons en mesure d'affirmer que nous disposons d'un système permettant d'organiser des élections de façon connectée. Une telle mesure ne serait de toute façon pas en ligne avec la réglementation européenne.

En tant qu'industriel, notre rôle est de déterminer si la technologie actuellement disponible nous permet d'« adresser » ces cas d'usage. Or nous y parvenons déjà dans d'autres pays et pas seulement en Estonie. De manière générale, tous les projets dans le monde doivent faire face à une certaine flexibilité. S'il est utile de disposer d'un cahier des charges initial, certains critères évolueront en fonction de l'actualité, comme c'est en ce moment le cas.

Les informations de base dont nous aurons besoin seront présentes sur la puce de la prochaine carte d'identité. Ces informations permettront de passer à des cas d'usage nettement plus critiques, comme les élections. Il sera toutefois nécessaire de légiférer pour y recourir.

**M. Philippe Latombe, rapporteur.** Il semble que les individus ne voient pas trop d'inconvénients à utiliser leur empreinte digitale pour déverrouiller leur téléphone, ou à présenter leur visage pour déverrouiller leur ordinateur. À l'inverse, à partir du moment où l'État souhaite récolter des données biométriques pour sécuriser l'identité de ces citoyens, un problème finit par se poser. Quel est donc votre point de vue sur la façon dont l'opinion perçoit le recours à la biométrie ?

**M. Pierre Lelièvre.** La biométrie est de plus en plus utilisée. Je pense donc que le niveau de confiance s'améliore. Le grand public est en tout cas en train de se familiariser avec des systèmes d'authentification biométriques. S'agissant du téléphone, les empreintes ont d'abord fait leur apparition, avant d'être suivies par la reconnaissance faciale.

Nous avons besoin de recourir à la pédagogie, ainsi que de mieux expliquer ce que nous souhaitons faire et comment nous comptons y parvenir. Sur ce point, il est essentiel d'établir une distinction entre l'identification et l'authentification. Un dispositif d'identification de masse au sein d'une population donnée sera perçu comme un système de surveillance, alors que l'authentification consiste à prouver qu'un nom correspond bien à une personne donnée. Pour leur part, les téléphones pratiquent essentiellement l'authentification et n'ont pas vraiment intérêt à recourir à l'identification.

Il existe trois niveaux de sécurité pour s'authentifier : ce que l'on possède, ce que l'on sait et ce que l'on est. Pour augmenter le niveau de sécurité, nous cherchons à associer toutes ces notions. Vous possédez ainsi un titre sécurisé dont la puce contient un certificat doté d'éléments cryptographiques permettant d'attester de façon certaine qu'il s'agit bien d'une carte du Gouvernement français. Cette carte peut également vous distribuer un code PIN. En entrant ce code, vous démontrerez que vous êtes effectivement la bonne personne ayant reçu la carte, comme c'est le cas dans le domaine bancaire. Enfin, le dernier niveau de sécurité est incarné par la biométrie, qui consiste à démontrer que vous êtes bien une vraie personne avec un visage en trois dimensions et que ce visage correspond au nom affiché.

La biométrie paraît assez largement utilisée aujourd'hui, que ce soit dans le monde du mobile ou dans la sphère gouvernementale, dans d'autres régions du monde. Il existe ainsi une question relative au téléphone et à la confiance accordée à l'État. Sur ce point, il est vrai que la défiance s'avère plus forte lorsqu'il est question de partager plus d'informations. Je ne sais pas si cette perception concerne l'ensemble des citoyens français ou si elle résulte simplement de certains lobbies. Toujours est-il que l'État demeure le mieux placé en la matière, car il dispose de plus d'informations, que n'importe quel acteur privé.

Certaines chaînes de grande distribution demandent des informations biométriques à leurs clients afin qu'ils puissent réaliser leurs achats. À titre personnel, je ne suis pas tellement favorable à de telles pratiques, car nous ne savons pas comment sont stockées ces données, comment elles sont protégées, ni qui peut y accéder.

La confiance entre le Gouvernement et la population ne se créera pas toute seule. Pour y parvenir, il sera nécessaire d'expliquer précisément pourquoi et comment les identités numériques seront gérées. Celles-ci ne seront peut-être pas destinées à des fins d'identification mais plutôt d'authentification, afin de permettre aux individus d'effectuer des transactions de façon plus sereine sur le web, par exemple pour accéder à des services ou pour vendre des objets.

La biométrie demeure donc un vrai enjeu. La question n'est plus de savoir si elle sera utilisée, car elle l'est déjà, mais quand elle le sera dans ce contexte.

**M. Philippe Latombe, rapporteur.** Chacun d'entre vous dispose à présent de deux minutes pour aborder un point qui n'aurait pas été évoqué et pour conclure.

**M. Pierre Lelièvre.** Je ne souhaite pas que le débat se cristallise sur la biométrie, qui est un moyen d'authentification présentant trois niveaux de sécurité, la puce correspondant probablement au plus élevé.

La question du niveau de maturité de la biométrie se pose, et pas seulement à l'échelle de la France. À l'heure actuelle, l'état de l'art montre que les algorithmes de biométrie ont environ une chance sur un million de confondre une personne avec une autre. De plus, la probabilité que le système échoue à identifier une personne donnée a été estimée à moins de 1 %. Le niveau de maturité de la technologie s'avère donc très bon.

Il convient désormais de nous demander comment nous souhaitons utiliser la biométrie dans le parcours client et dans notre vie de tous les jours en tant que citoyens, plutôt que de lutter contre elle. À condition de nous en donner les moyens, nous devons absolument nous équiper car nous sommes en train de perdre notre avance au profit d'autres acteurs.

**M. Olivier Charlannes.** M. Philippe Lelièvre a insisté à juste titre sur l'importance de pouvoir accéder aux données dans le développement des technologies d'Intelligence artificielle.

Il semble également judicieux, au niveau européen, de mettre en place un organisme d'évaluation de la performance de ces technologies, en opposition au *NIST (National Institute of Standards and Technology)*, l'organisme américain de référence. Pour l'instant, l'évaluation des différentes technologies est réalisée à l'aune de cet organisme. Ainsi, la mise en place d'un organisme comparable, au niveau européen, offrirait la possibilité à chaque État membre de s'y référer pour évaluer les technologies qui lui seront soumises, leur niveau de performance et la manière dont elles ont été développées. Cette mesure permettrait de disposer d'un vrai référentiel de comparaison au niveau européen, auquel les État membres pourraient avoir recours.

**M. Philippe Latombe, rapporteur.** Je prends ce point, afin d'étudier comment nous pourrions approfondir le sujet.

**M. Cosimo Prete.** La proposition de M. Olivier Charlannes peut être déclinée au niveau national. Nous pourrions ainsi nous doter d'une commission mixte composée d'experts de l'industrie et d'experts publics, afin de renforcer les ressources de l'ANTS dans le pilotage des programmes régaliens. Cette mesure permettrait de prendre de la hauteur par rapport au monopole d'État et de rationaliser les choix technologiques. Pour l'heure, ce monopole se trouve encore tiraillé entre source de profit et sécurité nationale.

Nous pourrions même envisager d'aller plus loin, avec la mise en place d'un *small patriot act,* afin de nous aider à bâtir une souveraineté nationale à l'échelle de l'Europe.

Il est toujours possible de mieux faire, mais qu'avons-nous fait de plus depuis la création en 2010 de la puce implémentée dans notre nouvelle CNIe ? Le pilote ne pourrait-il pas évoluer sans pour autant perturber les contraintes calendaires d'ici le mois d'août ?

*La séance est levée à 11 heures 05.*

## Membres présents ou excusés

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

Réunion du jeudi 1er avril à 9 heures 30

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