ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission des lois constitutionnelles, de la législation et de l'administration générale de la République

Mercredi
18 janvier 2017
Séance de 10 heures 30

Compte rendu n° 40

SESSION ORDINAIRE DE **2016-2017**

Présidence de M. Dominique Raimbourg, *Président*

ASSEMBLÉE NATIONALE

La réunion débute à 10 heures 40.

Présidence de M. Dominique Raimbourg, président.

La Commission procède à l'audition commune de M. Guillaume Poupard, directeur général de l'agence nationale de la sécurité des systèmes d'information (ANSSI), et de M. Henri Verdier, directeur interministériel du numérique et du système d'information et de communication de l'État (DINSIC), sur le traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

M. le président Dominique Raimbourg. Je remercie M. Poupard et M. Verdier d'avoir accepté notre invitation.

Cette audition fait suite à la publication au *Journal officiel* du 30 octobre 2016 du décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, dit « Titres électroniques sécurisés » (TES). Il prévoit l'enregistrement de données relatives au demandeur ou au titulaire du titre – identité, sexe, couleur des yeux, taille, domicile, filiation, image numérisée du visage et des empreintes digitales – sans dispositif de recherche permettant l'identification à partir de ces images ainsi que des informations relatives au titre lui-même, à son fabricant et aux agents chargés de sa délivrance. Il encadre les conditions dans lesquelles les personnes habilitées pourront accéder à ce système et prévoit le transfert des données d'ores et déjà enregistrées pour la délivrance des titres concernés.

Ce nouveau dispositif poursuit plusieurs objectifs : lutter contre la fraude et les usurpations d'identité ; simplifier les démarches des usagers ; améliorer l'efficacité et les coûts dans le cadre plus global de la réforme du service public. La création de ce fichier ayant suscité de nombreuses réactions, la commission des Lois a procédé, le 9 novembre 2016, à l'audition de M. Bernard Cazeneuve, qui était alors ministre de l'Intérieur. Un débat a eu lieu le 15 novembre dans l'hémicycle.

Le ministre de l'Intérieur avait indiqué avoir saisi pour avis l'ANSSI et la DINSIC, afin que ces deux organismes procèdent à un audit de sécurité du système TES, précisant qu'il s'engageait par avance « *à suivre scrupuleusement* » leurs avis. Le rapport a été remis hier au ministre de l'Intérieur, qui m'en a immédiatement adressé un exemplaire. Il a été mis en ligne sur le site du ministère, sous réserve d'une annexe couverte par le secret de la défense nationale. Un exemplaire vous a été envoyé par mail hier.

Le rapport conclut que le système TES est compatible dans son architecture et ses conditions d'usage à la sensibilité des données qu'il recueille. Pour autant, les auteurs formulent onze recommandations que le ministre s'est engagé à suivre.

La sécurité des systèmes d'information étant toujours sujette à discussion, une commission d'homologation se réunira sous un mois pour se prononcer sur l'analyse des risques et les moyens à mettre en œuvre pour mieux les maîtriser. L'ANSSI et la DINSIC restent associées. Le travail va donc se poursuivre, d'autant que plusieurs orientations, qui ont trait aux modalités de conservation des données biométriques et à l'opportunité de créer une base spécifique d'empreintes dédiée aux réquisitions judiciaires, sont en cours d'expertise.

Dans ce contexte, il m'a semblé utile que la Commission entende les responsables de l'ANSSI et de la DINSIC.

M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Nous allons d'abord, à tour de rôle, vous présenter nos deux organismes. L'ANSSI est une agence qui dépend du Premier ministre et qui est rattachée au Secrétaire général de la défense et de la sécurité nationale. Nous sommes en charge des questions de cybersécurité au sens large. En matière de prévention, nous nous intéressons en priorité aux administrations, à commencer par les plus sensibles, et aux opérateurs d'importance vitale. Nos capacités de détection d'attaques et de réaction sont régulièrement mises à contribution, même si nous n'en faisons pas forcément étalage. Nous employons beaucoup d'experts de toutes les questions qui touchent à la sécurité numérique, ce qui explique sans doute que nous ayons été chargés de cet audit sur le fichier TES, conjointement avec la DINSIC.

M. Henri Verdier, directeur interministériel du numérique et du système d'information et de communication de l'État (DINSIC). La DINSIC est également sous la tutelle du Premier ministre, placée au sein du Secrétariat général pour la modernisation de l'action publique. Nous sommes une sorte de direction des systèmes d'information (DSI) de l'État chargée de trois types de missions. En matière de gouvernance, nous devons donner un avis conforme sur tout nouveau grand projet au regard de sa trajectoire technique et financière et de sa faisabilité, pas sur les aspects de sécurité ou de la vie privée. En matière de mutualisation, nous nous efforçons de faire converger les DSI des ministères pour faire naître un service d'information unique pour l'État. En matière d'innovation, nous nous occupons de dossiers tels que ceux qui concernent *l'open data*, *l'open government*, etc. Autant dire que cet audit ne correspond pas aux missions traditionnelles de nos deux organismes.

Avant de répondre à vos questions, j'aimerais faire un propos liminaire pour insister sur trois points.

En premier lieu, pour reprendre la conclusion de notre court rapport, je dirai que les questions que vous vous posez aujourd'hui reviendront souvent dans de futurs débats. En quelques années, la biométrie s'est banalisée ; elle est entrée dans certains systèmes informatiques régaliens, mais elle est aussi utilisée par un nombre croissant d'entreprises – nous sommes quelque 600 millions à avoir laissé nos empreintes digitales à une entreprise de Cupertino… Elle est peut-être même entrée dans l'intimité des familles par le biais d'outils vendus notamment par quelques *startups* françaises.

Comme nous l'avons constaté dans le cadre de cet audit, il faut se poser des questions d'efficacité, de sécurité notamment vis-à-vis d'attaques extérieures, d'architecture système, de mode de circulation de la donnée, de gouvernance, de libertés publiques, etc. Une question était omniprésente : dans quel cadre de gouvernance faut-il s'inscrire ? Le débat, qui durera quelques années, devra produire une sorte de doctrine française de l'identité, de l'identification et de l'authentification. Cette question cruciale se posera pour d'autres fichiers. Il faudra être capable d'y apporter une réponse publique, débattue, argumentée. Elle devra émaner du législateur et du Gouvernement, et non pas d'agences techniques.

En second lieu, il faut signaler que l'audit s'est déroulé de manière remarquable : nos équipes ont été bien accueillies ; elles ont eu communication de toutes les pièces qu'elles avaient réclamées et réponse à toutes les questions qu'elles avaient posées. Ce qui va sans dire va encore mieux en le disant : nous avons eu toute liberté de rédaction pour formuler des conclusions sincères et étayées.

En troisième lieu, avant d'entrer dans le vif du sujet et en réponse à ce qu'on a pu lire dans la presse, je tiens à dire que ce fichier n'était pas sur une « trajectoire de dévoiement ». Des questions techniques précises nous sont certes posées le concernant : le fichier risque-t-il d'être dévoyé ou d'être attaqué avec succès par des *hackers* ? Nous allons essayer de répondre avec précision. En nous plongeant dans les archives, nous avons trouvé beaucoup de tentatives de remontées vers l'identité à partir de l'empreinte digitale. Pour faire une réforme qui va améliorer l'efficacité et les coûts du système de délivrance des titres, il a été décidé de prendre un outil robuste et éprouvé et de l'appliquer à d'autres usages – nous proposons quelques corrections pour ce faire. Cela ne signifie pas que le fichier était en passe d'être dévoyé par le biais de manœuvres en cours.

Après ces observations liminaires, sur lesquelles nous sommes d'accord l'un et l'autre, nous allons revenir sur les deux grandes questions qui nous étaient posées : la sécurité et le risque de dévoiement des usages du système.

M. Guillaume Poupard. Dans le domaine de la sécurité, nous nous inscrivons dans un contexte de menaces informatiques croissantes. C'est un lieu commun que de le dire mais, au sein de l'Agence, nous le vivons au quotidien, ayant à traiter différentes *fake teams*, avec des attaquants de plus en plus compétents et motivés qui peuvent être de grands États – nous pensons probablement aux mêmes sans avoir besoin de les citer. En cybersécurité, il est donc important de rester très modeste et de s'inscrire dans le temps.

Un système tel que TES pouvait être considéré comme sûr en 2008, mais huit ans c'est très long en cybersécurité. Il faut donc s'inscrire dans une dynamique et revoir en permanence la sécurité au vu des évolutions des techniques mais aussi de la doctrine. Ce que l'on pouvait conseiller en 2008 n'est pas ce que l'on conseille en 2016. Dans le cadre de l'audit, nous avons regardé très concrètement l'état de sécurité du système et de ses différents composants. Nous avons aussi pris en compte de nouvelles données qui n'étaient pas disponibles en 2008.

Les experts impliqués ont examiné les différents sous-systèmes ; ils ont cherché à savoir comment il était possible de détourner le système et d'en prendre le contrôle. Comme indiqué dans le rapport, nous avons découvert des vulnérabilités plus ou moins graves que nous n'avons pas décrites pour des raisons évidentes de sécurité du fichier. À l'ANSSI, nous n'avons pas l'habitude de rendre publiques les vulnérabilités que nous mettons au jour ; notre objectif est de nous assurer qu'elles sont bien prises en compte par le détenteur du système. Nous sommes dans cet état d'esprit avec le ministère de l'Intérieur et avec l'Agence nationale des titres sécurisés (ANTS). Nous leur avons transmis, au fil de l'eau, toutes les informations susceptibles de les intéresser. Je dois reconnaître que la prise en compte de la plupart de nos remarques a été extrêmement rapide et donc de nature à renforcer considérablement la sécurité du système.

Globalement, nos remarques sont de nature à élever la sécurité du système à l'état de l'art, comme l'on dit, que ce soit au niveau des points de collecte qui se trouvent la plupart du temps dans les mairies, au niveau du traitement qui s'effectue en préfecture, ou au niveau du stockage. Nous faisons des recommandations concernant l'usage de la cryptographie qui, vue de 2017, est insuffisamment présente. Nous proposons de renforcer notamment le chiffrement des bases de données et de durcir certains mécanismes.

Nous proposons aussi d'aborder la gouvernance en se plaçant dans une démarche d'homologation. Partant d'un système dont on a exprimé clairement les finalités, pour lequel

on a identifié des menaces et proposé des mécanismes de sécurité, l'autorité des entrées doit vraiment se faire expliquer quelles sont les vulnérabilités résiduelles. Dans ce genre de système, il n'y a pas de sécurité absolue. On peut toujours imaginer des sécurités supplémentaires et chercher des vulnérabilités résiduelles. Dans le cadre de cette commission d'homologation, il est important d'avoir tout cela en tête, afin d'être en mesure d'accepter ou de refuser d'homologuer l'utilisation du système.

Le ministère de l'Intérieur s'est donné un mois, ce qui est un délai raisonnable. Le ministre a également annoncé une révision annuelle de cette homologation, ce qui est plutôt ambitieux par rapport à ce que nous avons l'habitude de faire. Pour ma part, je m'en réjouis. Il s'agit de pouvoir bien suivre l'évolution de la sécurité de ce système dans le temps. Telle que nous l'avons perçue au cours de l'audit, la sécurité n'était pas du tout catastrophique mais elle était perfectible. Nombre d'améliorations déjà apportées vont s'inscrire dans le cadre d'un plan de durcissement de la sécurité. Surtout, le suivi va être fait dans la durée, ce que l'on préconise en général.

M. Henri Verdier. La question du dévoiement se pose à peu près dans les mêmes termes. À partir du moment où il existe une base de données contenant des informations, celui qui détient les clefs du code source peut démonter et remonter autrement le système. Il n'y a pas d'irréversibilité totale et éternelle d'un système informatique. C'est pourquoi nous proposons certaines mesures.

Il est possible, par exemple, d'élargir la gouvernance et de donner les clefs de chiffrement à deux ministères différents, qui n'ont pas forcément une grande habitude de coopération. Cela peut être intéressant.

Une grande question est posée dans le rapport et, à mon avis, elle demande quelques semaines de travail. À l'heure où nous parlons, on n'utilise pas les empreintes digitales pour établir les cartes d'identité. Il est possible de lutter contre la fraude grâce à des systèmes d'identification, mais nous recommandons d'examiner la possibilité de dégrader les informations utilisées pour bâtir cette sécurisation. Dans le rapport, nous envisageons une piste : ne stocker que des minuties, c'est-à-dire des points qui permettent de s'assurer, avec un très fort degré de probabilité, qu'une empreinte digitale est bien celle d'une personne, sans qu'il y ait un lien total et irréversible. Il y a quelques années, la Commission nationale de l'informatique et des libertés (CNIL) utilisait la notion de lien faible : une empreinte désigne une personne comprise dans un groupe de 1000, 2 000 ou 10 000 personnes répertoriées.

Il y a plusieurs manières de travailler avec une information moins précise pour bâtir une sécurisation des titres. Pour l'établissement des cartes d'identité, nous recommandons fortement de travailler avec une information moins précise que l'empreinte digitale complète. Pour l'établissement de passeports, la situation est différente dans la mesure où les conventions internationales et aussi une forme de consensus social poussent à l'utilisation des empreintes digitales : certains pays en font une condition d'entrée sur leur territoire ; quand il s'agit de franchissement de frontières, on accepte que l'État soit peut-être un peu plus régalien.

Mme Marie-Anne Chapdelaine. En préambule, je voudrais remercier le président de la commission des Lois d'avoir organisé l'audition de représentants de l'ANSSI et de la DINSIC, comme l'avait demandé mon collègue M. Luc Belot lors du débat sans vote qui a eu lieu à l'Assemblée nationale après la parution du décret du 28 octobre 2016. Je voudrais aussi

remercier M. Bernard Cazeneuve et le ministre de l'Intérieur M. Bruno Le Roux d'avoir rendu leur avis public.

Messieurs les directeurs, vos services ont été missionnés pour procéder à un audit de sécurité du système TES. Le rapport de cet audit, rendu public hier, constate que le système est compatible avec la sensibilité des données qu'il contient. Nous prenons acte de cette conclusion mais celle-ci ne nous rassure que partiellement : vos auditeurs ont aussi formulé onze recommandations afin d'apporter des améliorations et corriger des faiblesses.

Pour y répondre, le ministre de l'Intérieur annonce un plan d'action. Pouvez-vous nous affirmer que toutes vos recommandations seront prises en compte par ce plan ? Sinon, à quel degré le seront-elles ?

Comment va s'effectuer le contrôle de ce système au fur à et mesure de son application et de l'évolution des risques ? Le monde de l'informatique et du numérique est en mutation constante et accélérée. Les contrôles techniques sont essentiels, notamment pour le respect de nos libertés publiques. Comment s'assurer que la démarche d'homologation proposée par le ministre sera bien mise en œuvre ? Qui va la contrôler ?

De plus, vos services confirment nos inquiétudes quant au possible détournement du système à des fins d'identification, malgré toutes les précautions qui peuvent être prises par le ministère de l'Intérieur. Comme nous l'affirmions, vous rappelez également « *qu'il est impossible de garantir l'inviolabilité technique absolue d'un système d'information dans le temps* » et qu'il existe des risques inévitables. D'autres architectures techniques auraient-elles été mieux adaptées à ces risques ?

Certaines de vos recommandations retiennent mon attention. Dans la recommandation n° 1, vous affirmez que la centralisation des données biométriques pour la carte nationale d'identité a peu d'intérêt pour leur gestion. Pouvez-vous préciser ce constat, en revenant sur le lien faible et le gabarit des empreintes ? Ces dernières solutions sont-elles compatibles avec ce qui est en train de se mettre en place ? Sinon, que faudrait-il faire ?

La recommandation n° 2 concerne les réquisitions judiciaires. Quels seraient les risques de détournement des données traitées par TES et comment y pallier ?

Votre recommandation n° 4 m'inspire aussi quelques questions. Pour éviter les risques que peut induire l'intervention de sous-traitants, le système TES ne peut-il pas être développé et exploité en interne par des agents de la fonction publique dûment habilités ? Quelles autorisations pour quel accès ? Quelle homologation pour les éventuels sous-traitants ?

La recommandation n° 6 évoque la mise en œuvre du lien unidirectionnel. Sur le plan technique, qu'est ce qui garantit que le système d'accès aux données biométriques par ces liens unidirectionnels ne sera pas renversé ? Les filtrages seront-ils suffisamment opérationnels ?

Aucune structure n'est à l'abri d'intrusions pouvant totalement compromettre ce type de systèmes. Le phénomène du *hacking* a touché des multinationales spécialisées dans le numérique telles que *Yahoo* mais aussi des États comme Israël où la sécurité est une priorité absolue. Sommes-nous assez protégés contre une cyber-attaque ? Nos lois sont-elles adaptées aux cyber-attaques et à la cyber-défense ? D'autres systèmes ou architectures ne peuvent-ils

pas être envisagés afin de réduire au minimum ces risques inévitables ? Je pense à l'utilisation de fichiers décentralisés dans les pays de l'Europe du Nord.

Pour finir, je suggérerai au président de la commission des Lois qu'une audition annuelle de nos deux invités du jour et du ministre de l'Intérieur puisse être organisée sur ces questions qui me paraissent fondamentales pour la sécurité des citoyens, mais aussi pour leurs libertés.

M. Jacques Bompard. Notre pays multiplie toujours les structures quels que soient les dossiers traités, ce qui augmente les coûts et diminue l'efficacité. Alors que notre civilisation devient de plus en plus fragile en raison du développement de la mondialisation, dont les répercussions sont à la fois économiques et sécuritaires, ne devrait-on pas concentrer nos efforts ? La multiplicité des acteurs ne facilite pas la communication, déjà difficile à l'intérieur d'une même structure.

M. Joaquim Pueyo. En décembre dernier, monsieur Poupard, vous annonciez dans le journal *Le Monde* que « *des gens rentrent dans les systèmes d'information et préparent les attaques de demain, qui pourraient prendre la forme de sabotages ou de vols de données* » et que ces personnes « *préparent le terrain* » en cartographiant des systèmes d'information.

Alors que les cyber-attaques étaient jusqu'à présent motivées par l'espionnage économique, elles pourraient donc, à l'avenir, tendre à déstabiliser la France, comme vous l'expliquiez lors de votre audition conjointe au Sénat, à l'occasion de la mise en place du fichier TES. Vous évoquiez d'autres menaces, qui n'étaient pas classiques en 2008, comme la destruction du fichier par une organisation ou un pays étranger. Ce genre d'arme est de plus en plus utilisé dans le cadre de conflits avoués ou non entre grands États, indiquiez-vous.

Vos propos nous rappellent ce qui s'est passé lors des dernières élections présidentielles américaines. Pensez-vous que des faits similaires peuvent affecter les prochaines élections en France ?

Durant la même audition, monsieur Poupard, vous aviez estimé qu'un fichier comme TES allait « *attirer les convoitises, comme cela a déjà été le cas dans d'autres pays* ». La lecture de vos commentaires m'inspire une grande inquiétude. Pouvez-vous nous indiquer si les mesures sont prises et si les dispositifs actuels permettent de lutter contre de telles attaques, notamment celles qui viseraient à voler, corrompre ou détruire des données contenues dans des fichiers étatiques ?

M. Sébastien Pietrasanta. J'aimerais avoir une idée de la menace en matière de cyber-attaque. Vous avez bénéficié de moyens humains et financiers particulièrement renforcés. Dans une interview accordée au *Journal du Dimanche*, le ministre de la Défense M. Jean-Yves Le Drian indiquait récemment que les cyber-attaques subies par son ministère avait doublé pour atteindre le nombre de 24 000 en 2016 et qu'elles étaient de plus en plus sophistiquées. Ce constat corrobore votre propos introductif, monsieur Poupard.

L'année 2017 va être marquée par des échéances électorales. À l'automne dernier, vous avez reçu à l'ANSSI les responsables des différents partis politiques pour leur rappeler une nécessaire hygiène numérique, selon votre propre expression. Rappelons que les services secrets américains estiment que la Russie est à l'origine de la divulgation d'informations internes au parti démocrate lors des récentes élections présidentielles aux États-Unis. Qu'en

est-il en France ? A-t-on des inquiétudes concernant notre processus démocratique ? Avons-nous des éléments pouvant alimenter une éventuelle inquiétude ?

Nous pouvons aussi nous poser des questions à propos des données privées des partis politiques et des équipes de campagne. La protection des systèmes informatiques, qui coûte cher, n'est pas forcément une priorité pour les candidats à l'élection présidentielle, d'autant que les dépenses de campagne sont plafonnées, contrairement à ce qui se passe aux États-Unis. Peut-être faudrait-il réfléchir à faire sortir ce coût de la protection des données du montant plafonné des comptes de campagne.

J'aimerais aussi vous interroger sur le vote électronique qui concerne encore plus d'un million de Français, en dépit du moratoire imposé il y a quelques années et qui empêche de nouvelles communes d'adopter cette technique. Ne faudrait-il pas revoir la question pour les élections de 2017, tant que les risques d'intrusion informatique ne sont pas écartés ? Si les machines à voter ne sont pas connectées à internet, les logiciels qui exploitent les résultats du vote le sont et peuvent subir des attaques. Nous pouvons nous poser la question compte tenu de ce qui s'est passé aux États-Unis et de votre inquiétude manifeste, puisque c'est la première fois que l'ANSSI reçoit les principales formations politiques.

Profitant de votre présence, je voudrais vous dire que l'ANSSI aura un gros travail de sensibilisation à mener, à partir de juin et juillet 2017, auprès des parlementaires. Nous n'avons reçu aucune consigne en matière d'hygiène numérique à notre arrivée. Peut-être ne devrais-je pas le dire publiquement, mais les parlementaires sont vulnérables. Nous devons changer notre façon de faire avec l'aide de l'ANSSI.

M. Guillaume Garot. Monsieur Verdier, quels pourraient être les premiers fondements d'une doctrine française de l'identité ou de l'identification telle que vous l'avez évoquée, et comment la démarche de la France se situerait-elle par rapport à ce qui se pratique ailleurs, notamment aux États-Unis ?

M. Philippe Goujon. Je vous remercie, monsieur le président, d'avoir organisé cette audition, même si nous aurions souhaité aller plus loin. Beaucoup réclamaient, plutôt qu'un décret, une loi sur la protection de l'identité adaptée aux enjeux de sécurité actuels, qui se sont accrus depuis la loi de 2012 que j'ai rapportée. La France reste très en retard. Je remarque que le Conseil constitutionnel ne s'était pas prononcé, en 2012, pour ou contre la biométrie ni pour ou contre un fichier central, mais avait seulement considéré que certaines garanties prévues par cette loi étaient insuffisantes. Mais chacun sait que le Conseil sait adapter sa jurisprudence aux changements de faits et de circonstances...

Même si ce décret améliore l'authentification lors du processus de délivrance des titres d'identité et s'il modernise le fichier national de gestion pour la carte d'identité (FNG), tout à fait obsolète, je regrette que le Gouvernement renonce dans ce texte à appliquer plusieurs dispositions législatives qui n'avaient pourtant pas été censurées par le Conseil constitutionnel, telles que l'inclusion d'un composant électronique sécurisé, par exemple. Je déplore surtout que ce décret ne permette pas l'identification de personnes à partir des empreintes biométriques, ce qui aurait été bien utile à l'identification de cadavres – notamment de victimes d'attentats ou de catastrophes naturelles. L'impossibilité d'une telle identification limitera aussi les usages qui auraient pu en être faits par les services anti-terroristes.

Le rapport que nous avons reçu hier, fort tardivement d'ailleurs, soulève quelques questions. Que pensez-vous de la proposition, formulée par le ministre de l'Intérieur, de mise en place à moyen terme – conformément à une recommandation de la CNIL qui n'a pas été retenue jusqu'à présent – d'un système de conservation des données biométriques sous forme de gabarits ? Y a-t-il éventuellement un risque de confusion entre des personnes aux gabarits proches ? Si cette solution technique était retenue, que penseriez-vous de la proposition du ministre de créer une base spécifique d'empreintes dédiées aux réquisitions judiciaires ? En quoi un tel fichier de police judiciaire serait-il plus sûr pour la conservation de ces données sensibles, compte tenu du risque de piratage ? Quelles solutions technologiques recommanderiez-vous pour assurer aussi bien l'authentification que l'identification des personnes, en cas de besoin ? Vous avez évoqué très rapidement la base à lien faible, par opposition à la base à lien fort qui avait été retenue dans le précédent projet mais censurée au motif qu'il serait trop facilement possible de la consulter. Cette option mérite-t-elle néanmoins d'être étudiée ?

Ne risque-t-on pas, en suivant votre recommandation n°1 sur le chiffrement des données biométriques et la répartition de la clef d'accès entre plusieurs autorités, de compliquer la procédure d'accès et de ralentir ainsi certaines enquêtes qui nécessitent souvent un accès extrêmement rapide à l'information ?

Concernant, enfin, la sécurité du titre elle-même, le support de la carte d'identité est aujourd'hui tout à fait falsifiable, malgré son nom de « CNI infalsifiable ». Ne pensez-vous pas qu'une carte d'identité électronique devient aujourd'hui essentielle pour sécuriser matériellement le titre ? De même, le recours à la signature électronique pourrait constituer un moyen de protection supplémentaire intéressant dans nombre de domaines, notamment pour les achats électroniques.

M. Éric Ciotti. Comme souvent, certains jouent à se faire peur. L'audit que vous avez publié démontre en tous points que le fichier TES n'est en rien attentatoire aux libertés et que, bien au contraire, il est utile pour mieux protéger les libertés et lutter contre le fléau que constitue l'usurpation d'identité. Je veux redire le soutien que nous avons souhaité apporter à la constitution de ce fichier. La sécurisation des titres et la lutte contre l'usurpation d'identité faisaient partie des orientations qui avaient été fixées sous la précédente législature par la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), dont j'ai été le rapporteur. Ces orientations doivent aujourd'hui être confirmées et amplifiées. Ce fichier va donc dans le bon sens et les critiques qui lui ont été adressées me paraissent totalement inopportunes et largement infondées.

Nous devrions, et nous y serons sans doute contraints un jour, aller plus loin, notamment pour faire face à la menace terroriste à laquelle notre pays est confronté. Je regrette que ce fichier ne permette pas l'identification des personnes à partir des empreintes biométriques, ce qui serait un progrès très important. Je déplore également, comme M. Philippe Goujon, que la carte d'identité électronique ne soit toujours pas mise sur le métier alors qu'elle serait un très bon moyen de sécuriser matériellement les titres.

M. le président Dominique Raimbourg. Qu'est-ce exactement qu'une identification ? En quoi, l'identification présente-t-elle des dangers, pour certains, et des avantages, pour d'autres ? Le système mis en place représente-t-il une plus-value par rapport à l'actuel fichier existant ? Risque-t-on moins d'usurpations d'identité ?

M. Guillaume Poupard. L'authentification consiste à vérifier l'identité d'une personne à l'aide de ses empreintes digitales ou de ses données biométriques. L'identification est le procédé inverse. Dans le cadre de la sécurisation des titres, l'authentification présente un intérêt précis : elle permet de comparer les empreintes d'une personne faisant une demande de carte d'identité avec celles qu'elle aura laissées lors d'une demande antérieure. En ce sens, l'authentification prémunit davantage contre l'usurpation de titres. Elle n'empêche cependant pas les fraudes lors d'une première demande de carte d'identité, qui semblent majoritaires. Encore une fois, la sécurisation participe d'un ensemble de mesures.

Nous ne nous prononcerons pas quant à l'opportunité d'un fichier permettant de faire de l'identification, étant plutôt chargés de mettre en application les mesures que vous votez. Aujourd'hui, le fichier TES est plutôt axé sur l'authentification, raison pour laquelle nous recommandons, dans la lignée de la CNIL, de n'y conserver qu'une petite partie des informations. L'ensemble de l'empreinte n'est, en effet, pas nécessaire pour procéder à une authentification. Le système est un peu comparable à celui du code PIN d'une carte bancaire : nombre de personnes en France ont très probablement le même code à quatre chiffres sans que cela remette en cause la sécurité du système ni ne les empêche de s'authentifier. En revanche, on a besoin d'une image biométrique beaucoup plus précise pour pouvoir identifier avec une quasi-certitude une ou plusieurs personnes.

S'agissant de la prise en compte de nos recommandations, un plan d'action a été rédigé par le ministère de l'Intérieur avec lequel nous sommes en interaction étroite, dans de bonnes conditions. Nous ne sommes pas d'accord sur tout, et il y a beaucoup de discussions entre experts, qui sont fort intéressantes pour l'homologation puisque celle-ci consiste à mettre en regard les mesures prises, les risques et les menaces résiduelles. Inscrire cette homologation dans le temps, comme cela a été recommandé, permet de faire évoluer le niveau de sécurité du fichier et du système sous-jacent parallèlement à la menace et aux risques. Il serait contradictoire avec nos objectifs de sécurité de ne pas toucher à un système, même très bien conçu, au motif qu'il fonctionne. La démarche vertueuse qui est proposée par le ministère de l'Intérieur est clairement de nature à nous rassurer, et nous jouerons le jeu en assurant un suivi dans le temps de la sécurité du système.

Vous l'avez rappelé, aucun système n'est inviolable. Nous avons renoncé au concept de sécurité absolue pour lui préférer celui de sécurité dynamique, qui s'adapte au niveau de risque. On ne peut pas protéger tous les systèmes de la même façon. Ce serait même, pour des raisons économiques, totalement irréaliste. Mieux vaut avoir une vision claire de ce dont on veut se protéger. En l'espèce, compte tenu des risques de déstabilisation encourus, il me semble nécessaire de viser des attaquants au potentiel élevé. Certes, le niveau de sécurité attendu d'un tel fichier devra répondre à une exigence forte, mais il ne pourra toutefois pas atteindre la sécurité absolue. Tous les systèmes d'information, y compris les plus sensibles pour la sécurité nationale, tels les systèmes militaires, sont exposés au même risque d'intrusion. Simplement, la barre de protection est placée plus ou moins haut – parfois de manière très paranoïaque – en fonction des possibles attaquants, dans un jeu de calage entre la menace envisagée et les mesures techniques ou organisationnelles à mettre en œuvre pour s'en protéger.

S'agissant des autres architectures possibles, comme nous l'avons précisé en introduction de notre rapport, nous nous sommes interdits de les analyser. Cela ne veut pas dire qu'elles n'existent pas, mais la question qui nous était posée n'était pas celle-là : il s'agissait de déterminer si le système tel qu'il est peut être utilisé à court terme. La réponse est plutôt positive, moyennant les ajustements qui ont été faits. On pourrait, bien évidemment,

concevoir d'autres architectures plus décentralisées – certainement plus rassurantes, car plus faciles à sécuriser. Une base centralisée donne une impression de simplicité mais impose de telles mesures de sécurité que je ne suis pas certain que son coût final soit forcément inférieur à celui de bases décentralisées. Mais, encore une fois, nous ne voulons pas réécrire l'histoire, car les décisions qui ont été prises s'appuient sur une réflexion datant d'avant 2008. On procèderait peut-être différemment si on reprenait les choses aujourd'hui, mais je ne puis en dire davantage à ce stade.

Quant aux réquisitions judiciaires, elles sont légitimes. Nous avons seulement recommandé d'en avoir une meilleure traçabilité. On a besoin de savoir, en protégeant ces données par la suite, qui a accès à quelles informations. Certaines mesures techniques permettent de contrôler l'accès à ces informations, telles que les cartes à puce et certains moyens d'authentification. Mais il importe d'avoir plusieurs lignes formant une défense dite « en profondeur », de manière à pouvoir retrouver de manière fiable, le lendemain ou un an plus tard, quelle personne a interrogé la base à des fins judiciaires, quand et pourquoi. Une telle traçabilité est de nature à renforcer le contrôle que l'on exerce – y compris sur les personnes habilitées, car celles-ci peuvent subir des pressions ou être victimes de chantage. On a besoin de les protéger, parfois contre elles-mêmes. La traçabilité sert essentiellement à limiter la menace interne, car il n'y a pas que des attaquants extérieurs venant de l'autre bout du monde. La doctrine telle qu'on l'envisage aujourd'hui repose beaucoup moins sur une sécurité périmétrique – avec les « méchants » à l'extérieur et les « gentils » à l'intérieur. On ne fait plus confiance à grand monde, et l'on veut éviter d'avoir à faire confiance. D'ailleurs, quand on doit le faire, c'est qu'on ne peut plus faire autrement ; quelque part, c'est un échec. Dans les systèmes modernes, on évite autant que possible d'avoir à faire confiance.

La sous-traitance me semble nécessaire. On peut toujours rêver de ré-internaliser l'ensemble des systèmes d'information, mais je n'y crois pas, même si cela n'interdit pas d'avoir de bons informaticiens au sein de l'État – ce dont nous manquons à mon sens. Nous avons besoin d'une compétence en interne qui nous permette de sous-traiter efficacement. La sous-traitance suppose une bonne gouvernance et des contrats qui prennent en compte les questions de sécurité dans le temps même si, en faisant évoluer sa stratégie de sous-traitance dans le temps, on court le risque qu'il y ait « des trous dans la raquette ».

Le lien unidirectionnel pose une vraie question, à laquelle il faut répondre. Je serai un peu provocateur : s'il y avait collusion de plusieurs acteurs au sein du ministère de l'Intérieur, détenteur du système dans sa globalité, il serait tout à fait possible d'inverser le lien. Disposant de la liste de tous les noms et données biométriques ainsi que du moyen de les faire correspondre, il suffirait de relier ces données pour les 60 millions de personnes enregistrées dans le fichier pour reconstituer une base unidirectionnelle. Bref, si l'acteur menaçant est l'ensemble du ministère de l'Intérieur, la garantie du lien unidirectionnel ne tient évidemment pas. En revanche, face à des individus, nous disposons de moyens techniques permettant de limiter le risque qu'un opérateur du système, même légitime, fasse les 60 millions de requêtes pour reconstituer la base. En font partie la traçabilité et la détection de tout événement anormal, déclenchant un contrôle immédiat.

Nos lois sont-elles adaptées aux cyber-attaques ? De fait, la loi de programmation militaire de décembre 2013 a fait de la France un pays en pointe en matière de réglementation et de législation sur la cyber-sécurité, en prévoyant que les opérateurs d'importance vitale sont tenus de suivre des règles de sécurité fixées par le Premier ministre et par son bras armé, l'ANSSI. Cette disposition ne couvre, certes, que les opérateurs d'importance vitale et pas l'ensemble des systèmes sensibles, mais c'est déjà considérable. Cela inclut tous les grands

acteurs publics et privés des secteurs de l'énergie, de l'eau, des télécommunications et de la finance, soit tous les secteurs importants pour la sécurité nationale. Bien que difficile à appliquer, cette disposition est très vertueuse, et c'est la raison pour laquelle elle a été reprise par l'Allemagne ainsi que par la Commission européenne qui a élaboré une directive allant exactement dans le même sens. La France me semble donc bien préparée de ce point de vue, étant entendu qu'il convient toujours de maintenir un équilibre entre la force de la réglementation et le niveau de sécurité qu'on cherche à obtenir. Imposer à l'ensemble de nos concitoyens de faire de la sécurité, par exemple, n'aurait aucun sens.

M. Henri Verdier. Ayant lu des choses fausses dans la presse, je rappellerai quelle est l'architecture profonde du fichier TES. Ce dernier permet, à partir d'un nom, d'extraire de bases différentes fonctionnant en silo une empreinte digitale, une signature, une photo ou des informations alphanumériques – adresse, date de naissance et autres. Le lien permettant de retrouver une empreinte digitale, par exemple, est chiffré à l'aide de technologies déchiffrables pour qui a la clef.

Concernant les réquisitions judiciaires, on s'est rendu compte qu'un certain nombre d'usages ne visaient pas seulement à produire des documents mais qu'ils respectaient néanmoins toujours le sens prévu lors de la construction du fichier. Il a été dit, par abus de langage, que ce fichier avait été utilisé pour « identifier » des victimes ; en réalité, on y a eu recours pour aider des familles après certaines catastrophes, comme les attentats de Nice, mais toujours en allant du nom vers l'empreinte digitale. Le système peut, certes, être dévoyé mais pour autant que nous puissions en juger – après avoir posé la question une centaine de fois au cours de notre audit –, il a toujours fonctionné dans le sens prévu et seulement dans le sens prévu.

Vous avez abordé l'architecture de la sous-traitance. Le système a été élaboré en 2008 pour gérer les passeports, et plutôt bien pour autant que nous puissions en juger : le projet informatique a été tenu en temps et en heure et livré par une équipe resserrée, dans les limites du budget alloué. Reste que, pour mieux utiliser l'argent public, il a été décidé de diviser l'équipe opérationnelle en quatre fournisseurs. Puis la gouvernance du système s'est complexifiée, avec l'implication du ministère de l'Intérieur, d'une agence et de fournisseurs. Nous sommes arrivés, je crois, à un point où l'État va devoir réinternaliser certaines capacités – il n'a plus assez de grandes compétences informatiques. Il aura aussi besoin de s'entourer d'écosystèmes industriels de grande qualité. La vulnérabilité n'est pas liée à l'existence d'un fournisseur, elle survient lorsqu'on oublie qui est responsable de quoi et si l'on n'étend pas impitoyablement le champ de la traçabilité jusqu'au dernier salarié de tous les fournisseurs. Bref, une architecture avec fournisseurs se travaille.

Je n'ai rien à dire sur le risque de cyber-attaques lors des élections, car cette question ne relève pas de la DINSIC.

J'en profite néanmoins pour attirer votre attention sur un autre risque dont on parle trop peu. Vous avez tous remarqué la facilité avec laquelle on peut travailler sa e-réputation, certains parmi vous l'ont peut-être fait. Une toute petite agence travaille les liens hypertexte et les réseaux sociaux pour faire « monter » telle page sur *Google* ou sur *Youtube* et faire « baisser » telle autre. Il est facile de manipuler, sans recourir au *hacking* et à des informaticiens hors pair, l'image que ces sites renvoient du débat public en faisant monter outrancièrement certains articles, certaines informations mensongères ou vidéos. On ne regarde pas ce problème en face parce que ce n'est pas commode, dans une démocratie, d'imaginer regarder le contenu de la conversation. Il a fallu longtemps au législateur pour

bâtir le socle des lois Bichet et construire un équilibre entre la liberté de la presse et le pluralisme des opinions. On est un peu en panne quand cette question se pose sur la toile, et je pense que ce risque doit être pris en compte.

Il n'appartient pas aux experts techniques d'établir une doctrine française sur l'identité ou l'identification. Nous pouvons, en revanche, poser un certain nombre de questions auxquelles elle devrait répondre. Avons-nous la capacité d'établir nous-mêmes nos identités ou avons-nous perdu les technologies et les procédures pour le faire ? Sommes-nous interopérables avec ce que préparent les autres pays ? Le règlement eIDAS nous contraindra à accepter les identités des autres pays de l'Union européenne. Je n'exclus pas des formes de compétition d'identité numérique dans l'espace européen, certains faisant valoir la plus grande sécurité ou la plus grande souplesse de leur modèle. Regardez ce que fait brillamment l'Estonie. Il faut aussi penser cette doctrine en termes d'affluence, d'attractivité et de souveraineté.

Avons-nous inscrit dans l'architecture profonde des systèmes et leur gouvernance l'équilibre que nous souhaitons entre sécurité, vie privée et libertés publiques ? C'est dans les systèmes et les architectures que se déterminent ces grands équilibres-là. Il appartient à l'État de donner son arbitrage et de le traduire dans des systèmes.

Je crois que la carte d'identité numérique mérite d'être remise sur le métier. Pour notre travail d'audit, nous avons revu certains des acteurs des polémiques anciennes. Je ne suis pas sûr que les enjeux aient alors été parfaitement compris. La contestation, il y a une petite dizaine d'années, portait sur une carte d'identité numérique avec deux puces important beaucoup d'informations, une carte qui n'était pas seulement une carte d'identité. On a peut-être jeté un peu vite le bébé avec l'eau du bain. De nombreux acteurs de l'époque ne sont pas loin de le penser.

Autre question, avons-nous mis en place la gouvernance idoine pour organiser, piloter et superviser ces systèmes ?

Peut-être faudrait-il aussi, dans la définition d'une conception française de l'authentification, s'interroger sur les endroits où l'on ne veut pas avoir à s'authentifier. Voudriez-vous d'un monde dans lequel votre carte d'identité numérique pourrait vous être demandée à tout moment et dans lequel vous seriez obligés de prouver votre âge pour acheter un paquet de cigarettes – peut-être le déciderez-vous dans ce cas précis – ou pour toutes sortes de choses ? Doit-on réfléchir à des « poches » dans lesquelles l'authentification ne sera pas demandée ? Accorde-t-on la capacité de demander l'authentification au e-commerce ? Voilà des points qui devraient être abordés dans un grand débat public, articulés les uns aux autres – c'est ce qui est compliqué –, et peut-être pas fichier par fichier.

Nous l'indiquons dans le rapport, cette question se pose très profondément dans la sphère régalienne. Elle se pose un peu différemment dans la sphère de la simplification administrative, où l'on nous demande de pouvoir ne fournir des pièces qu'une seule fois, ou dans la sphère économique. Il faudra aussi articuler ces trois points de vue.

Je souscris à tout ce qu'a dit Guillaume Poupard. Je crois que la somme de nos interventions répond à presque toutes vos questions.

M. Guillaume Poupard. Je reviens sur les risques et menaces. C'est mon rôle que d'alerter sur ces risques qui sont bien réels. Le risque numérique ou informatique est parfois

connu sous l'angle qui n'est pas le plus grave – les attaques de sites internet sont désagréables mais pas graves fondamentalement pour la sécurité nationale. En revanche, le vol d'informations stratégiques est malheureusement aujourd'hui une réalité – ce n'est pas parce qu'on ne communique pas sur les victimes que cela n'existe pas. Le risque de sabotage est bien réel aussi – c'est tout l'objet du dispositif réglementaire qui est mis en place. Depuis les élections américaines, on s'intéresse de plus en plus aux risques de déstabilisation que l'informatique peut faire peser sur les processus démocratiques de nos pays. Cette menace ne doit pas nous tétaniser, elle doit être prise en compte au juste niveau, y compris dans le processus électoral que nous allons vivre. Ce processus reste très concret, avec des bulletins dans des enveloppes. C'est de nature à me rassurer. L'idée n'est pas de faire du numérique pour le plaisir de faire du numérique.

Je suis très favorable à l'extension du moratoire sur les machines à voter. Ces machines présentent le défaut d'être assez différentes les unes des autres ; elles sont difficiles à évaluer. Il faut peut-être se reposer la question de leur intérêt – mais c'est là un avis personnel –, en dehors de leur utilisation pour le vote des Français de l'étranger. Nous avons été associés au choix qui a été fait en 2012 du vote électronique concernant les élections législatives pour les Français de l'étranger. Depuis cinq ans, nous avons travaillé avec le ministère des Affaires étrangères parce que ce sont des systèmes compliqués et qui vont attirer les attaquants, cela ne fait aucun doute. Ces modalités de vote seront reconduites pour les élections législatives à venir. En toute franchise, je ne suis pas favorable au vote électronique, car lorsqu'on met en regard aujourd'hui les capacités de sécurisation dont nous disposons, même avec beaucoup d'efforts et l'intervention de gens très sérieux, et le niveau des attaquants potentiels, qui font probablement partie des meilleurs, il est difficile d'être totalement rassuré.

S'agissant des moyens, vous l'avez rappelé, l'ANSSI n'est pas à plaindre. Je suis, au contraire, très reconnaissant aux différentes autorités successives d'avoir pris en compte les questions de cyber-sécurité depuis la création de l'Agence en 2009 – le ministère de la Défense n'est pas oublié non plus. Le ministère compte 24 000 attaques, nous en dénombrons 20 000 parce que nous ne comptons pas la même chose. Il faut savoir ce que les chiffres recouvrent. Il est certain que les attaques sont de plus en plus nombreuses, les attaquants de plus en plus forts et les risques de plus en plus importants au fur et à mesure que notre société et notre économie se numérisent. Cela doit vraiment être un sujet de préoccupation aujourd'hui, mais aussi demain.

Il ne m'appartient pas de me prononcer sur l'exclusion des dépenses de sécurité des comptes de campagne, mais cela me paraît une évidence. Cette mesure permettrait d'encourager les partis politiques, dont la cyber-sécurité n'est pas le métier premier, à agir. Pour nous, les partis s'apparentent à des petites et moyennes entreprises (PME) dans leurs structures et leur équipement informatique. Il faudrait pouvoir les inciter, et avec eux les autres structures de même type, à investir dans la sécurité, sans que cela se retourne contre eux.

Certains ont retenu du vif débat que la carte nationale d'identique électronique a suscité il y a quelques années que cette carte n'était pas possible. Or toutes les auditions que nous avons menées et toutes les expertises montrent que ce n'est pas le cas. Je suis convaincu qu'une carte intégrant des moyens modernes – certes coûteux – tels que des puces serait de nature à apporter de véritables protections, comme c'est le cas pour les passeports. Je vais plus loin, je considère que c'est peut-être même le rôle de l'État de fournir une identité électronique à chaque citoyen. Il s'agit typiquement d'une activité régalienne, de mon point

de vue, mais, là encore, cela nécessite un débat que l'on ne peut pas tenir ici en quelques minutes.

M. Sébastien Huyghe. Quel est l'état de la réflexion dans un domaine dans lequel la fraude massive est avérée, celui de l'assurance-maladie ? On sait que l'impression de la photographie de l'assuré sur la carte Vitale n'a pas fait la preuve de son efficacité ; la location de cartes à l'heure ou à la journée est un phénomène répandu, qui contribue à une utilisation à mauvais escient de l'argent public. Est-il envisagé d'insérer dans la carte Vitale des données telles que l'empreinte digitale ? Ce serait le meilleur moyen de lutter contre la fraude en permettant aux professionnels de santé de vérifier que le porteur de la carte en est bien le titulaire.

Mme Françoise Descamps-Crosnier. Je remercie les deux directeurs pour leurs interventions, qui ne nous ont pas complètement rassurés. J'ai néanmoins entendu qu'il était impossible de garantir une sécurité intégrale du système. Du coup, m'adressant à notre président, je m'interroge, comme Mme Marie-Anne Chapdelaine, sur l'opportunité de procéder à une évaluation annuelle de notre dispositif de sécurité numérique ?

M. Jean-Yves Caullet. Vous avez évoqué l'hypothèse qu'un jour le système pourrait être mis en défaut à la suite d'une attaque. Le mode dégradé est-il prévu dans les systèmes de sécurité ?

M. le président Dominique Raimbourg. Je réponds à la question de Mmes Chapdelaine et Descamps-Crosnier. Le prochain rendez-vous n'aura pas lieu dans un an mais à l'issue de la commission d'homologation : nous procéderons peut-être, alors, à une audition du ministre de l'Intérieur. Si nous sommes hors session, nous demanderons au ministère de nous transmettre les conclusions de la commission d'homologation et je vous les ferai parvenir.

S'agissant de l'année prochaine, je pourrais vous dire que je vais tout faire pour être réélu et redevenir président de la commission des Lois. Mais les prédictions sont un exercice des plus difficiles. Le Parlement a la possibilité de s'emparer de n'importe quel sujet relevant du contrôle de l'action publique. Si la minorité souhaite s'intéresser à cette question, elle dispose d'un droit de tirage pour la création de commissions d'enquête dont les pouvoirs d'investigation sont importants.

M. Guillaume Poupard. Une remarque préalable avant de répondre. On évoque aujourd'hui le fichier TES, mais il existe une multitude de fichiers et de systèmes sensibles. Il importe d'appréhender ces questions dans leur globalité. L'exercice auquel nous nous sommes livrés pourrait donner des idées de réévaluation de certains autres fichiers qui détiennent parfois beaucoup plus d'informations sur un plus grand nombre de citoyens.

Le technicien peut vous répondre qu'on sait considérablement réduire la fraude, mais ce sont des choix qui ne relèvent pas de lui. Il s'agit de déterminer où placer le curseur sur la précision dans l'identification des personnes ou sur le croisement des différents fichiers. Si on veut lutter contre la fraude, les possibilités sont multiples. Certains géants du numérique nous montrent à quel point, en croisant les informations, on peut obtenir un ciblage extrêmement précis des individus. Comme le disait M. Henri Verdier, il ne faut probablement pas aller trop loin dans ce sens. Il faut fixer un curseur entre la sécurité, la lutte contre la fraude et la protection des libertés. Ce n'est pas à moi de faire la leçon.

M. Sébastien Huyghe. J'ai été membre de la CNIL. Une solution qui ne porte pas atteinte aux données personnelles consisterait à introduire dans la puce de la carte Vitale l'empreinte digitale, sans qu'elle sorte de la carte.

M. Henri Verdier. Lorsque le débat s'ouvrira sur des sujets tels que la sécurisation de la carte Vitale, il faudra qu'y soit versée toute la variété des choses subtiles que sait faire l'informatique. On peut sortir de la métaphore du gendarme et du voleur et penser autrement qu'avec une base centrale. On peut faire des choses réversibles, du *privacy by design* ; on peut activer les choses avec le consentement de l'utilisateur ; on peut stocker des informations en périphérique ou sur deux systèmes différents qui ne marchent que lorsqu'ils sont réconciliés. Il va falloir s'interroger sur les concepts de *cloud* personnel, de *vendor relationship management,* de système complètement distribué, de passage du monde physique au monde virtuel... Si nous ne considérons pas la palette des outils disponibles, nous allons créer des systèmes qui seront déjà archaïques, des métaphores d'une époque révolue. On peut même convoquer des identités de nature différente suivant le contexte ou laisser le soin à l'usager de déterminer celles qu'il veut utiliser à un instant déterminé. Il faudra faire preuve d'un peu de finesse numérique.

S'agissant de la réversibilité du système, l'empreinte digitale est quelque chose de très particulier. Si vous la perdez, c'est à vie ; si vous vous la faites voler, c'est pour toujours. C'est l'une des raisons pour lesquelles nous proposons de travailler sur des gabarits, sur des versions dégradées de l'empreinte. S'il fallait un jour reconstruire un autre système, on pourrait ainsi s'appuyer sur d'autres points de l'empreinte. La perte des empreintes brutes est non seulement grave pour la vie privée, mais elle signifie aussi la renonciation à divers usages biométriques pour longtemps.

M. le président Dominique Raimbourg. Je vous remercie, messieurs, pour votre disponibilité.

La réunion s'achève à 11 heures 50.

Informations relatives à la Commission

La Commission a désigné :

— *M. François Pupponi,* rapporteur sur le projet de loi ratifiant les ordonnances du 21 novembre 2016 n° 2016-1561 complétant et précisant les règles budgétaires, financières, fiscales et comptables applicables à la collectivité de Corse, n° 2016-1562 portant diverses mesures institutionnelles relatives à la collectivité de Corse et n° 2016-1563 portant diverses mesures électorales applicables en Corse ;

— *M. Guillaume Larrivé,* rapporteur sur la mise en application de la loi qui serait issue de l'adoption du projet de loi relatif à la sécurité publique ;

— *M. Guy Geoffroy,* rapporteur en vue de l'audition de M. Daniel Hochedez, dont la nomination à la fonction de membre de la Haute Autorité pour la transparence de la vie publique a été proposée par le Président de l'Assemblée nationale.

Membres présents ou excusés

Présents. - M. Ibrahim Aboubacar, Mme Nathalie Appéré, M. Christian Assaf, M. Luc Belot, M. Jacques Bompard, M. Jean-Yves Caullet, Mme Marie-Anne Chapdelaine, M. Éric Ciotti, M. Jean-Michel Clément, M. Gilbert Collard, M. Sergio Coronado, M. Marc-Philippe Daubresse, M. Jean-Pierre Decool, Mme Françoise Descamps-Crosnier, Mme Sophie Dion, M. Philippe Doucet, M. Olivier Dussopt, M. Georges Fenech, M. Hugues Fourage, M. Guillaume Garot, M. Guy Geoffroy, M. Bernard Gérard, M. Philippe Goujon, Mme Françoise Guégot, M. Philippe Houillon, M. Sébastien Huyghe, Mme Nathalie Kosciusko-Morizet, M. Jean-Christophe Lagarde, M. Guillaume Larrivé, M. Jean-Yves Le Bouillonnec, M. Olivier Marleix, Mme Sandrine Mazetier, M. Paul Molac, M. Pierre Morel-A-L'Huissier, M. Edouard Philippe, M. Sébastien Pietrasanta, M. Pascal Popelin, M. Joaquim Pueyo, M. François Pupponi, M. Dominique Raimbourg, M. Alain Tourret, Mme Cécile Untermaier, M. Daniel Vaillant, M. Jacques Valax, M. Patrice Verchère, Mme Marie-Jo Zimmermann, M. Michel Zumkeller

Excusés. - Mme Marie-Françoise Bechtel, Mme Huguette Bello, M. Gilles Bourdouleix, M. Patrick Devedjian, M. Marc Dolez, Mme Laurence Dumont, M. Daniel Gibbes, M. Yves Goasdoué, M. Philippe Gosselin, Mme Maina Sage, M. Roger-Gérard Schwartzenberg, M. François Vannson, M. Jean-Luc Warsmann, Mme Paola Zanetti

Assistaient également à la réunion. - Mme Pascale Crozon, M. Michel Ménard