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
14 janvier 2021
Séance de 9 heures 30

Compte rendu n° 20

SESSION ORDINAIRE DE **2020-2021**

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

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, réunissant des représentants d'entreprises, avec M. Yoann Kassianides, délégué général de l'ACN, Mme Louise Bautista, représentant M. Mathieu Isaia, directeur général de TheGreenBow, M. Arthur Bataille, président de Silicom, fondateur de Seela, M. Jacques de La Rivière, président et cofondateur de Gatewatcher, et M. Sébastien Garnault, fondateur de la CyberTaskForce et de Paris Cyber Week, président de Garnault & Associés

La séance est ouverte à 9 heures 30.

Présidence de M. Jean-Luc Warsmann, Président.

M. le président Jean-Luc Warsmann. Avant toute chose, j'exprime mes meilleurs vœux à chacune et chacun, au terme d'une année 2020 des plus difficiles.

Nous reprenons les travaux de notre mission d'information par deux tables rondes. Elles se consacrent à la souveraineté numérique et à la commande publique. En échangeant avec des acteurs publics et privés, notre objectif consiste à voir comment la commande publique peut être mise au service, d'une part de la transformation numérique de nos administrations, d'autre part de la construction d'une forme de souveraineté numérique nationale ou européenne.

Pour la première table ronde, sont présents par visioconférence M. Yoann Kassianides, délégué général de l'ACN, Mme Louise Bautista, représentant M. Mathieu Isaia, directeur général de TheGreenBow qui ne peut participer aux échanges de ce jour, M. Arthur Bataille, président de Silicom, fondateur de Seela, et M. Jacques de La Rivière, président et cofondateur de Gatewatcher. M. Sébastien Garnault, fondateur de la CyberTaskForce et de Paris Cyber Week, président de Garnault & Associés, assiste également à la réunion.

Je les remercie des réponses écrites qu'ils nous ont d'ores et déjà adressées ou pour celles qu'ils nous feront encore parvenir.

M. Philippe Latombe, rapporteur. Je m'associe aux vœux du président pour l'année 2021. J'espère que nous sortirons rapidement de l'état de crise sanitaire et que la mission d'information sera en mesure de reprendre ses travaux autrement qu'à distance.

À titre d'introduction de la présente table ronde, je souhaite en interroger les participants sur plusieurs sujets.

Pouvez-vous d'abord nous préciser ce que recouvre pour vous la notion de souveraineté numérique ? Elle fait l'objet d'une attention croissante de la part des pouvoirs publics depuis le commencement de la crise sanitaire. En raison de son caractère ouvert, nous en avons entendu plusieurs définitions au cours des différentes auditions que nous avons déjà menées. Certains la rapprochent d'une forme d'autonomie stratégique ou décisionnelle. Le regard que vous portez, en tant qu'acteurs privés, sur ce concept nous intéresse. Vous nous préciserez comment vous pensez qu'il peut se traduire concrètement dans les politiques publiques.

J'aborderai ensuite la commande publique, objet direct de notre table ronde. Il s'agit d'un outil puissant puisqu'il représentait près de 87,5 milliards d'euros en 2019, selon le baromètre de l'Assemblée des communautés de France (AdCF) et de la Banque des

territoires. Estimez-vous que la commande publique se tourne assez vers des solutions numériques et technologiques françaises ou européennes ? Certaines de ces solutions étant portées par des petites ou moyennes entreprises (PME), nous aimerions savoir si les PME, ainsi que les entreprises de taille intermédiaire (ETI), parviennent à accéder suffisamment et facilement à la commande publique. Dans le cas contraire, vous nous indiquerez quelles difficultés elles rencontrent.

Enfin, nous évoquerons avec vous l'enjeu de la numérisation des entreprises, particulièrement prégnant depuis le déclenchement de la crise sanitaire. Nous formulerons ici deux interrogations principales. En premier lieu, comment inciter les entreprises à se numériser davantage, c'est-à-dire à recourir à des outils numériques qui leur permettent d'être plus compétitives ? En second lieu, devant un risque croissant, comment développer une culture de la cyberprotection chez les acteurs privés ? M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a récemment confirmé l'augmentation exceptionnelle du nombre des attaques informatiques en 2020, de même qu'il en a souligné l'inventivité des auteurs.

Je vous cède la parole.

M. Jacques de La Rivière, président et cofondateur de Gatewatcher. Depuis une dizaine d'années, la commande publique relative au numérique constitue en France un sujet récurrent. PME et grands groupes français du numérique accèdent à cette commande par le moyen de centres d'achats généralisés, telle l'Union des groupements d'achats publics (UGAP). La difficulté se révèle essentiellement culturelle. Les acheteurs publics ne donnent pas automatiquement leur préférence aux produits numériques français. À contraintes comparables du point de vue des marchés publics, ceux d'autres pays européens, comme l'Allemagne, choisissent spontanément les produits nationaux, avant que d'envisager le recours à des solutions d'origine étrangère. En France, l'acheteur public s'oriente souvent d'emblée vers l'offre américaine. Elle lui paraît mieux garantir son projet. Il faut changer cette approche.

Des initiatives à l'instar de celle que la direction interministérielle du numérique (DINUM) a engagée en faveur d'un nouveau label, vont en ce sens. Ainsi que vous l'avez rappelé, la commande publique ne manque pas d'importance en raison de son volume. Elle est appelée à se renforcer encore du fait de la crise qui sévit. Vecteur d'innovation, source de développement des produits, elle s'avère essentielle pour les PME.

Quinze ans en arrière, lorsque l'entreprise de commerce en ligne Amazon a lancé son offre de services informatiques via internet, ou *cloud computing,* elle a bénéficié, de la part de ses autorités nationales, pendant les deux premières années, d'une commande publique de 600 millions d'euros. Par comparaison, lors de son lancement en France en 2012, Cloudwatt n'a obtenu que l'attribution d'un seul projet public, celui du réseau national de télécommunication pour la technologie, l'enseignement et la recherche (RENATER), pour un total de 200 millions d'euros d'investissement. Cette offre d'hébergement en ligne française a finalement échoué.

Par ailleurs, le personnel de l'administration française tend souvent à redévelopper par ses propres moyens des produits numériques nationaux déjà existants sur le marché. De la sorte, il concurrence ces mêmes produits. En l'absence de mutualisation, de tels développements engendrent de plus des coûts particulièrement élevés. De nombreux exemples existent.

Mme Louise Bautista, TheGreenBow. Sur le premier point soulevé, celui de la définition de la souveraineté numérique française ou européenne, et à côté d'autres interprétations possibles, je perçois fondamentalement deux approches complémentaires. La première met en avant l'intelligence économique. Elle permet d'intégrer les grands groupes stratégiques, ainsi que les PME, au cercle de la souveraineté numérique. La seconde se concentre sur le secteur public et la continuité du service public.

Aujourd'hui, l'inquiétude principale a d'abord trait au risque de ne pas être en mesure d'assurer la continuité du service public. Le cas de figure s'en présenterait si des plateformes numériques étrangères décidaient d'interrompre leurs prestations. Il pose la question de notre indépendance politique sur la scène internationale. Pour l'heure, afin d'assurer la continuité du service de l'État, nous sommes dépendants de fournisseurs numériques extérieurs et à tendance monopolistique.

À celui de la continuité du service, la notion d'intelligence économique ajoute des critères relatifs à la création d'emplois et à l'accroissement du pouvoir d'achat au sein de l'État.

La formulation d'une critique négative ne saurait prévaloir uniformément. Sur les aspects d'audit et de certification des produits numériques de sécurité, à l'instigation de l'ANSSI à l'échelle nationale et de l'Union européenne à celle du continent, force est de constater une indéniable progression. Les efforts dans le sens d'une homologation des produits permettent d'assumer un début de souveraineté numérique française et européenne.

S'agissant de la commande publique, je reviens, à la suite d'un précédent entretien que nous avons eu, sur l'arsenal juridique existant. Nous disposons de l'instruction générale interministérielle (IGI) n° 1300 et de ses classifications. Dans le respect du droit de la concurrence européen, elle autorise l'apposition d'une mention « Spécial France » lors des appels d'offres inhérents à des commandes publiques.

Les récents échecs relatifs aux commandes publiques de la Banque publique d'investissement (Bpifrance) ou de Health data hub (HDH) montrent combien il fut préjudiciable de n'y pas recourir, particulièrement du point de vue de la protection des données de santé des citoyens. Par comparaison, je doute que, dans ce dernier domaine éminemment stratégique, l'Obamacare (*patient protection and affordable care act*, loi sur la protection des patients et les soins abordables, promulgué en 2010) ait seulement envisagé de recourir à la solution française d'hébergement d'OVHcloud.

Il n'apparaît pas indispensable de légiférer davantage. Utilisons les outils juridiques en vigueur. Au moment des appels d'offres, la mention « Spécial France » implique de ne retenir que des sociétés françaises dans des domaines qui comportent un enjeu de nature stratégique pour la Nation. Ces outils s'appuient sur le travail efficace que les autorités de certification, au premier rang desquelles l'ANSSI en France, assurent depuis plusieurs années.

En revanche, pourquoi ne pas étendre le champ des obligations actuelles en prévoyant celle d'utiliser des produits certifiés pour les identités publiques ou les opérateurs d'importance vitale (OIV) ?

L'adoption du règlement général sur la protection des données (RGPD) a montré le lien entre efficacité des textes et crainte de la sanction pécuniaire. Dès lors, je suggère que

nous disposions d'une autorité pleine et entière, avec un budget dédié, qui sanctionne ceux qui ne respecteraient pas les dispositions de cet arsenal juridique que j'évoquais.

M. Yoann Kassianides, délégué général d'ACN. Je souscris aux propos que les deux précédents intervenants ont tenus, tant sur les problèmes qui se posent que sur les avancées que nous relevons.

Organisation professionnelle, l'ACN représente les entreprises de la filière de la confiance numérique en France. La filière de la confiance numérique renvoie notamment à l'identité numérique et à la cybersécurité. Elle se révèle des plus présentes, vivaces et performantes en France. Elle a généré quelque 13 milliards d'euros de chiffre d'affaires en 2019. Elle comprend de nombreuses entreprises, dont des numéros un mondiaux, des ETI, de jeunes et petites entreprises innovantes (*startups*). Elle dispose d'un véritable savoir-faire. Il convient de ne pas l'oublier. L'attention tend à se centrer sur le seul marché du numérique grand public où, de fait, les acteurs français sont moins présents. Ce seul constat ne saurait conduire à tirer la conclusion de leur absence totale du secteur du numérique.

Au sein de l'ACN, une vision large de la notion de souveraineté prévaut. Nous l'entendons d'abord comme le pouvoir suprême reconnu à une nation. Ce pouvoir implique une compétence exclusive sur un territoire donné. À l'évidence, la définition se complexifie en matière numérique. Dans ce domaine en effet, la notion même de territoire apparaît plus difficile à cerner. Une certaine agilité intellectuelle et juridique s'avère nécessaire pour y transcrire le concept traditionnel de souveraineté.

Nous livrant à ce travail, nous aboutissons à assimiler la souveraineté numérique nationale, d'une part, à la capacité pour un État à exercer ses attributions de souveraineté dans l'espace numérique, d'autre part, à sa faculté à utiliser et à protéger contre d'éventuelles attaques des moyens numériques propres qui autorisent cet exercice. En d'autres termes, nous retenons la possibilité pour l'État d'employer des outils numériques au service de ses prérogatives régaliennes.

Quoiqu'étendu, cet ensemble conceptuel demeure opérant. Il permet de regrouper toutes les actions et conclusions utiles à la préservation de la souveraineté nationale.

Pour l'échelle européenne, pertinente de nos jours compte tenu de la concurrence internationale et de la dimension des blocs tant économiques que géostratégiques en présence, nous préférons, à l'ACN, employer l'expression d'« autonomie stratégique ». Celle-ci nous paraît mieux préserver la logique juridique. Nous ne perdons pas de vue que traditionnellement le droit réserve le concept de souveraineté aux seules entités étatiques. L'Union européenne ne revêt pas la qualité d'un État au sens strict. Divers traités internationaux lui ont plutôt délégué une partie des prérogatives de ses États membres.

Comment la notion de souveraineté numérique, ainsi que son pendant d'autonomie stratégique, se traduisent-ils ?

Dès lors qu'il exerce des missions régaliennes de manière numérique, il importe que l'État veille concomitamment à disposer des outils appropriés et à conserver l'exclusivité de sa compétence.

À titre d'exemple, je citerai l'identité et l'état civil. La transposition numérique de l'état civil pose une difficulté. Nous remarquons que de nombreuses identités cohabitent dans

le domaine numérique. Parmi elles, les plus pertinentes ne sont pas celles que les États européens contrôlent.

Si l'État entend poursuivre sa mission déterminante d'identification de ses ressortissants, le sujet de l'identité numérique devient central. Des travaux en ce sens se poursuivent. Leur résultat devra se matérialiser à brève échéance, tant les acteurs privés qui, la plupart étrangers, développent leur propre identité numérique, progressent avec célérité. Les outils permettant d'exercer des prérogatives régaliennes sont à considérer prioritairement.

Une autre manière de préserver la souveraineté nationale ou l'autonomie stratégique européenne consiste à s'appuyer sur des acteurs à la fois disponibles et performants.

Il convient de plus que l'État entretienne une vision stratégique. Elle suppose la mise en cohérence de l'ensemble des actions qui relèvent du numérique, au regard de la sécurité, de la confiance et de la souveraineté.

Le numérique reste encore trop diffus. Nous le retrouvons dans toutes les applications et interactions sociales et économiques. Chaque sujet spécifique dispose encore de ses propres développements numériques et d'un traitement local. Un effort de cohérence s'impose. Le numérique, la confiance dans le numérique, constituent des axes d'attention prioritaires. Les affrontements à venir s'effectueront dans le domaine numérique. Pour l'État, prendre l'initiative requiert ici une exigence de transversalité et d'homogénéisation. Une vision de surplomb, un niveau décisionnel adéquat, doivent nous garder de l'actuelle dissémination des décisions, assurément contreproductive.

Dans l'initiative publique, la question de la souveraineté numérique prend toute sa place quel que soit le secteur d'activité considéré. Elle semble d'emblée évidente en matière de défense ou de sécurité nationale. Elle apparaît de prime abord moins nettement dans d'autres domaines de l'action publique mais ne s'y impose pas moins. À notre avis, et peut-être sous forme d'études d'impact, l'attention à la souveraineté mérite de concerner tout processus de décision ayant trait au numérique. En ce sens, nous la rapprocherions des préoccupations d'ordre environnemental, elles-mêmes nécessairement transversales et impliquant une étude préalable des effets des décisions à prendre. Une approche de ce type nous aurait évité bien des désagréments et débats.

En dernier lieu, lorsque l'État se comporte en qualité d'acheteur, il se doit de faire montre d'exemplarité. Il s'agit évidemment qu'il se conforme aux préoccupations de souveraineté numérique, mais encore qu'il s'assure, au-delà de la seule origine nationale du produit acheté, que l'action qu'il mène aide à conforter une filière par nature stratégique puisqu'elle lui apporte les outils à même de maintenir sa souveraineté en conservant la maîtrise de son espace numérique. Outre la prise en compte de la nationalité du produit, l'État s'attachera par exemple à l'existence d'un environnement connu et de confiance, ou simplement à celle d'un approvisionnement interchangeable, sans tension ni contrainte.

Vous l'aurez compris, le message que nous entendons porter devant vous consiste d'abord à ce que la considération de la souveraineté embrasse l'ensemble des initiatives publiques qui comprennent une dimension numérique ; c'est-à-dire vraisemblablement toutes les actions publiques, tant nous imaginons mal que cette dimension en puisse désormais être absente.

M. Arthur Bataille, président de Silicom, fondateur de Seela. La société Silicom est une société de conseil. La société Seela propose, en partenariat avec Airbus, une formation en cyberentraînement. Elle a elle-même fondé un groupement, FIRST (French Industrials for Resilience, Security & Trust), qui promeut les enjeux de sécurité sous l'angle des outils, de la formation et de l'acculturation des entreprises, principalement à destination des ETI et PME.

Je partagerai avec vous les enseignements de mon expérience en tant que dirigeant de PME.

La crise sanitaire nous a permis de nous forger une vision claire de l'état actuel du numérique en France et, en particulier, de son niveau de développement au sein des entreprises françaises. Au cours de cette crise, nous avons été confrontés à une élévation significative des attaques, tant en nombre qu'en qualité. Elles ont perturbé des entreprises françaises dans leur modèle économique.

À mon sens, la souveraineté numérique concerne également les entreprises françaises, ainsi que les collectivités territoriales. Elle interroge la capacité de résistance de nos entreprises dans leur création de valeur ajoutée, dans leur recherche de développement, dans la défense des actifs dont elles disposent, notamment en matière de propriété intellectuelle.

Nous concentrons généralement notre attention sur les OIV. L'ANSSI surveille de près les risques d'attaques susceptibles de les affecter. L'Agence nationale pour le numérique (ANPN) leur garantit un certain niveau de sécurité. En revanche, nous ne nous préoccupons pas assez des sous-traitants des grands groupes et des administrations. Eux aussi hébergent des données.

Indépendamment de considérations qui prôneraient l'utilisation des seuls produits français ou européens, il convient de relever un problème de maîtrise des techniques numériques. En qualité de dirigeant d'une société de conseil, je m'interroge sur la capacité de la France à former ses jeunes des universités et des écoles d'ingénieurs dans les domaines de la sécurité informatique. Nos formations se focalisent par trop sur des métiers dits généralistes. Elles ne spécialisent pas assez.

Au contraire, les filières de formation par alternance paraissent répondre mieux aux problématiques et enjeux actuels dans ces domaines. En dépit du cursus généraliste que j'ai moi-même suivi, celui des classes préparatoires et des grandes écoles d'ingénieurs, sur le constat de son manque de pragmatisme, j'embauche plus favorablement des alternants. Leur première expérience professionnelle les amène à développer une expertise véritablement technique.

Certes, administrations, ministères et grands groupes entretiennent les moyens de maintenir en toute sécurité la capacité opérationnelle de leurs systèmes d'information. En revanche, à l'occasion de la crise sanitaire, souvent les directeurs des systèmes d'information (DSI) des PME ont dû mettre en place des outils de communication à distance, des réseaux privés virtuels (*virtual private networks*, VPN), sans réellement savoir ni comment les administrer, ni bénéficier d'équipes formées à ces produits.

En matière numérique, la question de la formation continue, particulièrement à l'aide d'organismes tels que les opérateurs de compétences (OPCO), me paraît posée. Je la juge fondamentale. Sauf erreur, je ne pense pas que des appels d'offres aient été publiés ces derniers mois qui viseraient à accompagner les entreprises dans la formation de leurs

collaborateurs. Je soutiens que de cette formation dépend en partie la défense de notre souveraineté numérique.

M. Philippe Latombe, rapporteur. Mme Louise Bautista, j'aimerais revenir sur vos propos. Vous avez évoqué les exemples des appels d'offres de Bpifrance et de HDH. La mission d'information consacrera une audition aux données de santé et entendra les représentants de HDH. Elle a d'ores et déjà auditionné ceux de Bpifrance. À la suite de réponses similaires que nous avions précédemment reçues de la part d'autres intervenants, ils nous ont expliqué avoir choisi de recourir à Amazon Web Services (AWS) car cet acteur propose à ce jour la meilleure qualité de service du marché, avec la suite logicielle la plus aboutie. Ils en soulignaient une avance d'une ampleur telle qu'elle semblait exclure toute solution française ou européenne, à l'exception peut-être, moyennant quelque temps, de Gaia-X.

Ce sentiment revêt-il une dimension culturelle, ainsi que, M. Jacques de La Rivière, vous le suggériez ? L'acheteur public préfère-t-il d'emblée, sans autre examen, une solution américaine à une offre française ? Au contraire, existe-t-il entre elles une différence de niveau si marquée que le choix ne peut autrement s'orienter ?

Une autre question s'adresse à M. Arthur Bataille, sur les aspects de formation. Il se dit communément que la filière française ne manque pas de reconnaissance, pour ce qui touche notamment à la cybersécurité, à l'identité et à la confiance numériques. Pourquoi n'obtenons-nous pas une meilleure diffusion dans les entreprises et les administrations des connaissances de nos spécialistes dans ces domaines ? Quel échelon fait-il défaut ?

Mme Louise Bautista. Je dirai après M. Yoann Kassianides qu'imposer en toutes circonstances, dans le choix de produits informatiques, un simple critère de nationalité ne prendrait guère de sens. Nous ne saurions exclure des considérations d'excellence. Poser une obligation de choisir systématiquement une solution française ne favoriserait pas la qualité de l'offre nationale.

En revanche, l'apposition d'une mention « Spécial France » s'avère pertinente dès lors que nous constatons un enjeu crucial pour la Nation, la présence de données qui lui sont stratégiques. Dans ces conditions, le choix du meilleur produit devient secondaire. La considération de l'autonomie stratégique devrait toujours l'emporter sur le poids des argumentaires certes efficaces de commerciaux, par exemple ceux d'Amazon, qui savent mettre en avant auprès des administrations les fonctions et applications évoluées de leurs solutions d'hébergement des données. Le choix se circonscrirait alors aux offres nationales d'OVHcloud et d'Outscale. Quoique moins étendues sans doute que celles de leurs principaux concurrents étrangers, elles s'avèrent de qualité et propres à répondre aux besoins auxquelles nous les destinerions.

Je ne porte aucune accusation à l'encontre de Bpifrance. Des faiblesses, des pressions et des discours commerciaux interfèrent dans la prise des décisions. En pareille occurrence, j'estime néanmoins que le choix de recourir à une plateforme étrangère ne devrait pas être ouvert. Il appartient au législateur d'intervenir. Amazon est une entreprise américaine. La France est membre de l'OTAN et évidemment l'alliée des États-Unis. Les deux États n'en sont pas moins des concurrents. Concevrions-nous de nous adresser à la Corée du Nord ou à la Chine, afin de bénéficier de leurs solutions numériques ? Nous ne leur confierions certainement pas les données de nos entreprises les plus prometteuses dans le domaine des techniques de pointe, les « licornes » de demain. Pourquoi y consentir avec une société

américaine ? Je doute qu'une entreprise telle qu'Airbus, fort bien consciente des enjeux de l'intelligence économique, accepterait de seulement l'envisager.

M. Philippe Latombe, rapporteur. Quand nous interrogeons Bpifrance ou d'autres acteurs, nous en recevons une réponse qui tend à amoindrir la portée du risque au motif que les données demeurent continûment chiffrées et que la clé de chiffrement leur appartient en propre. En aucun cas, nous disent-ils, l'hébergeur, qu'il s'agisse d'Amazon, de Microsoft Azure ou de n'importe quel autre, n'en dispose. Dans le cas précis de Bpifrance, l'autorité de certification compétente, l'ANSSI, a validé le choix de recourir à AWS. De nouveau, je m'interroge sur la possibilité d'un problème d'ordre principalement culturel.

M. Arthur Bataille. M. le rapporteur, vous avez précédemment utilisé le terme de « diffusion ». Je défends avec ferveur la qualité de notre industrie et de nos ingénieurs français. Néanmoins, en matière numérique, nous nous confrontons à une évolution extrêmement rapide des techniques à l'œuvre. Elle s'accélère sans cesse, au service d'un monde lui-même en perpétuel changement. Les principes, les procédures et les moyens de la sécurité des systèmes d'information qui étaient valables trois ans plus tôt sont déjà révolus. La problématique de la sécurité informatique n'est pas récente. La première attaque sur un réseau en ligne remonte à 1989.

Notre difficulté consiste donc à adapter rapidement nos programmes pédagogiques à la réalité, aux outils et aux enjeux. Je réitère que la formation en alternance présente ici un avantage certain. S'effectuant en entreprise, elle imprègne les étudiants de cette réalité, de ces outils et enjeux actuels.

Par ailleurs, je ferai état du danger de la précipitation de la commande publique. La nécessité de bénéficier d'une solution à brève échéance conduit à pencher vers la solution la plus aisément accessible. Vous avez mentionné la question du chiffrement des données. Ses enjeux s'avèrent complexes et souvent peu maîtrisés techniquement. Thomas Baignères, fondateur et président de l'entreprise Olvid, pourrait en témoigner. La clé de chiffrement n'offre pas une sécurité absolue. La détenir en exclusivité ne donne pas l'assurance d'une parfaite sécurisation des données et de leur inaccessibilité par un tiers.

Je partagerai avec vous une anecdote personnelle. L'un des responsables informatiques de l'entreprise que je dirige, qui en a élaboré tout le réseau intermédiaire, a pu un temps penser que l'intégralité de nos données étaient cryptées du fait qu'elles ne circulaient que selon un mode binaire, en interne entre nos différents sites.

Dans les débats qui nous animent, le constat reste le même, quoique à une échelle bien supérieure. Les techniques actuelles ont pris une envergure telle que nous n'en maîtrisons la portée ni la façon dont elles sont utilisées.

Mme Louise Bautista. Au sujet des clés de chiffrement, au centre de la réponse de Bpifrance, je renverrai à une autre audition que votre mission d'information parlementaire a organisée et dont j'ai pris connaissance. Il s'agit de celle de M. Charles Thibout, tenue le 12 novembre 2020. S'appuyant sur un rapport d'experts militaires mandatés par le ministère de la défense en 2008, au moment d'évaluer un projet que Microsoft avait présenté, votre interlocuteur commençait par rappeler que nos services de sécurité nationaux avaient alors établi que la pratique dite des « portes dérobées » (ou *backdoors*) dans les logiciels qui portent sur des données stratégiques, et quand bien même ils émanent d'alliés, était courante. Rien ne garantit jamais contre le risque de cette pratique, même la possession en propre de clés de

chiffrement. Celle-ci n'assure aucunement de l'intégrité et de la stricte confidentialité des services.

Un second risque a trait à la maintenance de l'hébergement des données numériques et à la continuité du service public. Un différend toujours possible, y compris avec un allié – tel celui qui émergea au début des années 2000 entre la France et les États-Unis au sujet du veto que la première menaça d'opposer contre une nouvelle guerre en Irak –, pourrait amener le fournisseur à interrompre sa prestation. Parmi d'autres, une réponse de cette nature revêtirait la forme d'une arme diplomatique. Ses conséquences ne seraient pas anodines. L'hypothèse n'en est certainement pas à considérer avec légèreté.

M. Jacques de La Rivière. Dans le domaine du numérique, la France compte des acteurs de premier plan sur la scène internationale, des « champions ». Je pense par exemple à Atos, Capgemini ou Sopra Steria. Cependant, ils ne proposent qu'une offre de services. Nous avons par ailleurs échoué s'agissant des produits.

La raison en tient au marché local. Sous l'effet d'un cercle vicieux, ce marché commandant essentiellement des produits américains, ainsi qu'en témoigne le choix de Bpifrance, au moment de la mise en place des prêts garantis par l'État (PGE), de s'adresser à Amazon, les offreurs français ou européens n'y disposent pas d'un volume de commandes suffisant pour exister face à la concurrence étrangère et proposer un niveau de fonctionnalités équivalent.

Au contraire, en matière de prestation de services informatiques, outre un vrai soutien à l'export, les acteurs français bénéficient notamment des spécificités du droit du travail national. Ne souhaitant pas embaucher directement et rester en mesure de changer de ressources, les donneurs d'ordre leur font prioritairement appel.

S'agissant des produits informatiques, aucune dynamique réglementaire n'intervient. Seules sont à relever d'occasionnelles prescriptions que l'ANSSI émet sur la robustesse des produits. Certaines ont par exemple pu intéresser les sondes de détection des OIV que Gatewatcher élabore. Néanmoins, en l'absence d'obligations réglementaires systématiques sur la certification des produits, à même d'en garantir la robustesse et par suite de répondre aux exigences de la souveraineté, nous resterons confrontés à l'offre massive de produits étrangers.

Pour mon entreprise, j'ai bénéficié d'un PGE. À cette occasion, j'ai constaté la simplicité d'utilisation de l'application informatique qui se rapporte au dispositif. Les champs à remplir tiennent en une unique page en ligne. N'importe quel hébergeur pouvait prendre en charge cette application et les données qu'elle génère, avec ou sans clé de chiffrement. OVHcloud, Outscale, ainsi que la multitude des hébergeurs indépendants qui existent en France et en Europe, en avaient la capacité. Néanmoins, pour des raisons de facilité, parce qu'ils sont d'abord formés sur des produits américains, les développeurs de l'application des PGE de Bpifrance ont choisi de s'orienter, sans autre interrogation, vers ce qu'ils connaissaient le mieux, l'offre d'AWH.

Mme Louise Bautista. Je partage sans réserve ce qui vient d'être dit. Nous comptons en effet en France des champions du numérique. Nous ne le devons cependant pas uniquement à nos talents. Historiquement, le plan gouvernemental Calcul que le président Charles de Gaulle a lancé en 1966, avec les financements d'entreprises qu'il emportait, y a également fortement contribué. Il a permis le développement d'entreprises telles qu'Atos,

Bull, France Télécom, devenue Orange, Capgemini, ainsi qu'une myriade de PME, dont TheGreenBow pour laquelle je travaille. Une initiative, une impulsion politique majeure a rendu possible ces réalisations.

Désormais, un ministère du numérique, un arsenal juridique renforcé et des mesures concrètes seraient nécessaires. Au-delà des paroles, nous attendons des acteurs politiques qu'ils favorisent un nouvel et indispensable élan. À tous les niveaux, les compétences existent. Nous avons évoqué les produits de sécurité. Dans ce domaine, TheGreenBow réalise du chiffrement depuis vingt-deux ans, y compris pour des sociétés américaines. Les exemples de réussites et de reconnaissance mondiale sont nombreux. Nous disposons de belles entreprises, de startups innovantes, d'excellentes écoles. Il ne saurait être question d'entretenir un quelconque complexe d'infériorité. Seule une impulsion nous manque.

M. Philippe Latombe, rapporteur. Selon vous, comment procéder ? Doit-il s'agir d'une initiative strictement française, avec un ministère dédié et un plan spécifique, ou l'échelon européen vous semble-t-il mieux approprié ?

Mme Louise Bautista. Les deux niveaux français et européen doivent se combiner. Certes, nous ne saurions rien entreprendre sans l'Europe, notamment en matière de certification. En revanche, pour certains projets, notamment ceux qui touchent à l'intelligence économique, dans des domaines où nous pourrions avoir des concurrents européens, sur des sujets qui mettent en cause la continuité de l'État, une souveraineté numérique française demeure incontournable. Elle se traduit par exemple par la mention « Spécial France ».

Trop attendre de l'Europe constituerait un écueil. En dépit de l'énergie que déploie le commissaire européen au marché intérieur, M. Thierry Breton, il nous faut également promouvoir le changement à l'échelle nationale. L'un ne va pas sans l'autre.

M. Arthur Bataille. Si un ministère du numérique se forme, il importe qu'il ne limite pas son intervention aux aspects réglementaires et au RGPD. La problématique dont nous traitons revêt une dimension essentiellement technique.

J'apprécierais que des groupes de travail ministériels évaluent l'état précis de la situation. Nous devons également renforcer les moyens de l'ANSSI. Il s'agit d'accompagner les entreprises françaises dans la préservation de la sécurité de leurs infrastructures et de poursuivre la mise en place de procédures de sécurité à l'usage des collectivités territoriales.

À l'échelle de l'Union européenne, le partage des connaissances et des compétences apparaît par ailleurs déterminant si nous entendons aboutir à l'élaboration d'une structure souveraine de *cloud*. La crise sanitaire porte aujourd'hui un coup d'arrêt fâcheux au programme d'échange des universités européennes. Il est fondamental qu'il puisse reprendre à brève échéance.

En tout état de cause, les principaux acteurs de l'industrie ou de la banque françaises déploient leurs ramifications dans le monde entier. Les considérations tenant au numérique ne sauraient se restreindre au seul territoire national.

Enfin, du point de vue de notre souveraineté, je soulignerai l'importance des plans d'actions qui s'appuient sur le crédit d'impôt recherche. Je remercie les pouvoirs publics de continuer à financer ainsi la recherche française, en réservant les aides accordées aux entreprises nationales.

M. Yoann Kassianides. Je souscris à l'idée selon laquelle il convient de mêler les deux niveaux français et européen.

La question de la souveraineté numérique se pose avec acuité du fait de l'omniprésence de produits d'origine américaine ou asiatique. La crise sanitaire a mis en lumière notre dépendance à ces produits. Elle a aussi provoqué une prise de conscience générale. Chacun mesure désormais la nécessité d'assurer notre souveraineté par nos propres moyens.

Devant les blocs majeurs qui se sont constitués, la menace apparaît d'un ordre géopolitique et géostratégique. La réponse ne peut être strictement française. L'échelle pertinente est celle de l'Europe.

Pour autant, il ne s'agit nullement de dénier toute possibilité d'initiative nationale. Du fait de l'excellence de ses entreprises, de sa recherche, de son expérience dans le domaine de la sécurité numérique, la France conserve des atouts de taille. Rappelons que l'invention de la carte à puce lui revient. Elle possède des compétences reconnues mondialement en matière de sécurisation et de chiffrement. Il nous appartient de nous appuyer sur ces atouts et de les porter au niveau européen.

Un tel niveau s'avère cohérent. Les membres de l'Union européenne partagent un même système de valeurs. Nous ne l'affirmerions pas s'agissant de la Chine, ni même des États-Unis. La première fonction des outils de confiance numérique vise à nous permettre de déployer nos activités dématérialisées conformément à notre système de valeurs. Ils sont les garants de ces valeurs quand il s'agit de le transposer dans le monde numérique.

De plus, la pertinence de l'échelle européenne se révèle sous l'angle économique. Revenons à la question de la certification. À ce jour, au sein de l'Union européenne, vendre un produit soumis à des obligations de certification impose encore de s'adresser, tour à tour, à chacune des autorités nationales de certification compétentes. Cette contrainte entraîne une complexité et des coûts supplémentaires non négligeables. En comparaison de la situation de leurs principaux concurrents internationaux, elle constitue un frein au développement économique des acteurs européens.

L'Union européenne s'attache à lever de telles barrières. En 2019, le *cybersecurity act* a ouvert la voie de certifications valables dans l'ensemble de l'Union. Nécessairement long, le processus de discussion se poursuit autour de critères communs. Il contribuera à définir un espace économique et numérique européen comparable aux blocs concurrents dont nous faisions état. Il se révèle primordial pour les entreprises européennes qui développent des produits numériques. Elles doivent pouvoir s'appuyer sur un marché domestique équivalent à ceux de leurs concurrents les plus actifs.

Enfin, des prérogatives régaliennes demeurent l'apanage des États. Elles ne relèvent pas de la compétence de l'Union européenne. Elles maintiennent l'utilité d'une souveraineté numérique nationale.

La combinaison des deux échelons, ceux de l'État et de l'Union, doivent s'harmoniser intelligemment. Assurément, la France se trouve en position de jouer un rôle de « pilote ». Sa filière numérique et son autorité de certification, l'ANSSI, jouissent de la reconnaissance de ses partenaires européens. Elles ont vocation à servir d'exemple. Il faut les y encourager. Les

entreprises françaises en tireraient un avantage certain dans la conquête du marché numérique européen, s'il se concrétise.

Il revient donc à l'État d'élaborer une vision unifiée et de faire montre de la volonté d'obtenir un socle national fort, pour le porter à l'échelle de l'Europe, à même ensuite d'en assurer une diffusion plus large.

M. Philippe Latombe, rapporteur. Sans intention polémique, j'aimerais connaître le regard que vous portez sur la DINUM et sur son rôle. Sa création entendait précisément harmoniser l'action de l'État dans le domaine du numérique. Jugez-vous que la DINUM influence efficacement la commande publique qui s'y rapporte ?

M. Jacques de La Rivière. Au sein de la DINUM, la mission Label élabore actuellement un label destiné à la commande publique française. Il orientera les décideurs vers l'achat de solutions nationales ou européennes. Même tardive, l'initiative en paraît bonne. Elle contribuera au changement progressif de la culture de l'achat public qui, pour l'heure, se tourne prioritairement vers des offres étrangères.

Mme Louise Bautista. J'estime que l'élaboration d'un label appelé à éclairer les commandes publiques constitue une excellente nouvelle. Elle marque une évolution nette par rapport à ce qui a prévalu quelques années auparavant. Je pense notamment au recours à l'application Tchap, de conception britannique, quand des *startups* nationales, telles qu'Olvid, offraient des solutions au moins équivalentes, avec une qualité de chiffrement irréprochable.

Par ailleurs, bien que TheGreenBow s'emploie à sécuriser les connexions de télétravail des agents du secteur public et assure, par conséquent, une mission des plus stratégiques actuellement, j'ai peu eu affaire à la DINUM. Il m'a fallu m'adresser à chacun des ministères concernés.

M. Philippe Latombe, rapporteur. Au nom de TheGreenBow, vous avez donc entretenu des relations ministère par ministère ? Nous expliquez-vous qu'aucune réflexion globale ne s'est engagée sous l'impulsion de la DINUM ?

Mme Louise Bautista. Je vous le confirme. Néanmoins, nous n'avons pas essuyé de fin de non-recevoir auprès de la DINUM. Simplement, lorsque le premier confinement a commencé, différents ministères nous ont joints et nous en avons appelé d'autres. Nous avons lancé une opération intitulée « le VPN français ». Nous proposions une offre à un tarif préférentiel aux collectivités territoriales ainsi qu'aux établissements publics. Nombreux sont ceux qui nous ont sollicités, sans que la DINUM n'intervienne. Cependant, l'opération s'effectue depuis lors dans des conditions tout à fait satisfaisantes.

M. Yoann Kassianides. Nous mettons ici le doigt sur une difficulté centrale du sujet de la confiance numérique. La propension de chaque « verticale », qu'il s'agisse des ministères ou des secteurs d'activité, consiste à traiter en interne les questions qui l'intéressent, en l'occurrence celle de la numérisation.

Introduire une part de transversalité, qu'elle soit interministérielle au niveau national, interétatique au plan européen, ou encore intersectorielle, s'avère assurément complexe à réaliser. Une solution homogène, applicable uniformément, relève de la gageure. Tout secteur, tout domaine, chaque verticale, comprend des spécificités. Nous ne pouvons les ignorer. Je

laisse de côté les questions de chapelles et de prérogatives que chaque verticale aura tendance à défendre pour les conserver. Les sujets stratégiques imposent de les dépasser.

Il faut tendre à une certaine proportion de transversalité et chercher, du moins, à l'accroître. Sont positives les initiatives qui, d'une manière ou d'une autre, y contribuent. Celles de la DINUM comptent parmi leur nombre. L'équilibre reste à trouver entre transversalité, effort d'homogénéisation, d'une part, et personnalisation nécessaire à chacune des verticales, d'autre part.

Pour l'heure, nous constatons que l'ensemble des questions de sécurité et de confiance numériques se traitent d'une façon verticale.

Mme Louise Bautista. Si mon entreprise n'a pas entretenu de relations avec la DINUM, je tiens en revanche à souligner une initiative du secrétariat d'État chargé du numérique. Au commencement du confinement, ce secrétariat d'État a mis en place une page internet comportant la liste des entreprises françaises du numérique – *startups*, PME, grands groupes – qui souhaitaient répondre par des offres de solidarité à la numérisation contrainte de l'économie. La page répertoriait l'opération de TheGreenBow, « le VPN français », et lui a permis, ainsi qu'à d'autres acteurs, de distribuer gratuitement un nombre élevé de licences.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder d'autres aspects ?

M. Arthur Bataille. Je soulèverai cinq points qui me semblent mériter l'attention de la représentation nationale.

Il s'agit d'abord d'aider et de subventionner universités et écoles en France, afin qu'elles aillent plus avant dans leur démarche pédagogique. Nos établissements d'enseignement doivent disposer de moyens et outils à la mesure des enjeux. Ils souffrent durement de la crise sanitaire qui impose l'éloignement de leurs étudiants.

Nous suggérons ensuite d'augmenter le montant des budgets alloués à la formation dans les entreprises. Une politique résolue doit inciter les entreprises à former leurs collaborateurs.

De plus, nous encourageons la création d'un groupe de travail sur les enjeux de souveraineté numérique et les technologies à valoriser en France, voire en Europe. Il réunirait opportunément les experts de la direction générale de l'armement (DGA) du ministère des armées et ceux de l'ANSSI.

M. Philippe Latombe, rapporteur. En somme, vous évoquez la création d'un équivalent de la *defence advanced research projects agency* (DARPA), l'agence du département de la défense des États-Unis.

M. Arthur Bataille. Nous disposons en France de compétences précieuses au sein de différents ministères sur les aspects techniques des métiers du numérique.

J'ajoute la nécessité de subventionner la recherche, de même à la hauteur des enjeux que nous nous fixons. Je regrette que nous déterminions aujourd'hui les subventions à l'aune de la création de valeur ajoutée par les entreprises et non en fonction du coût réel que la recherche représente pour elles.

Enfin, nous appelons de nos vœux la mise en place d'un plan européen en vue de la conception d'une plateforme en ligne qui exposerait l'offre disponible de produits numériques européens.

M. Philippe Latombe, rapporteur. Je prends note de vos cinq propositions.

Mme Louise Bautista. Je souhaite à mon tour vous en soumettre cinq autres.

Générale, la première invite à passer des paroles aux actes. Nous entendons de nombreux propos fort intéressants. Il s'agirait de les mettre, au moins pour une partie d'entre eux, en pratique. La présente table ronde se déroule par visioconférence. Je note qu'il nous faut à cette occasion utiliser l'application Zoom, une application américaine. Or, utiliser un outil de visioconférence souverain ne relève pas de l'impossible, ni seulement du très difficile. En France, des entreprises certifiées par l'ANSSI, comme Tixeo ou Private Discuss du groupe lyonnais PIMAN, le permettent sans rien céder sur la qualité du service.

La deuxième reprend l'une des premières idées que j'ai précédemment présentées. Elle concerne la création d'une instance de contrôle. Celle-ci aurait pour fonction de faire respecter, sous peine d'amende, l'obligation de certification des produits, ainsi que l'application de la mention « Spécial France » lors des appels d'offres. La proposition suppose de légiférer. La perception du montant des amendes serait susceptible de compenser la dépense liée au budget à consacrer à la nouvelle structure.

La troisième proposition revêt un caractère social. Lorsque j'observais que nous disposons en France des compétences utiles en matière de cybersécurité, j'omettais de signaler qu'elles n'offrent pas exactement l'image d'un modèle de mixité. De fait, les femmes ne représentent qu'environ 11 % de l'effectif total de la filière en France. À un stade décisif, nous nous passons fâcheusement d'un réservoir de talents supplémentaires. Certains pays asiatiques ou Israël ont lancé de vastes initiatives destinées à attirer un nombre plus élevé de femmes vers les métiers de la sécurité. Nous serions bien inspirés de les imiter dans cette voie.

Une quatrième proposition a trait à la sensibilisation à la cybersécurité et aux enjeux d'autonomie stratégique ou de souveraineté numérique, non seulement des établissements d'enseignement supérieur et des professionnels, mais encore des élus, aussi bien locaux que nationaux. Constatant que Google a engagé des initiatives en ce sens à l'attention des PME, je précise plaider en faveur d'une sensibilisation par un ou plusieurs opérateurs français.

Enfin, à la suite d'une tribune publiée à ce sujet, la cinquième proposition que je porte défend la création d'un ministère du numérique. Elle semble recueillir le consensus des acteurs français du secteur. Ni un secrétariat d'État ni une direction interministérielle ne suffisent. À l'approche de la présidence française de l'Union européenne, se doter d'un ministère de plein exercice prendrait de plus valeur d'exemple.

M. Philippe Latombe, rapporteur. Je partage vos réserves au sujet de l'application Zoom. Je suis le premier à en regretter l'utilisation pour nos auditions et tables rondes. Nous incitons autant que nous le pouvons le service informatique de l'Assemblée nationale à changer rapidement d'outil.

M. Jacques de La Rivière. Je me permets de signaler que la *startup* française Livestorm propose également une solution de remplacement à Zoom. D'un emploi des plus

simples, elle fonctionne de manière parfaitement satisfaisante. Elle permet à l'utilisateur de créer lui-même ses liens de connexion pour des réunions à distance de type conférence téléphonique ou conférence en ligne (webinaire), sans passer par son service informatique. Si vous le souhaitez, nous nous tenons à votre disposition pour vous accompagner dans le choix d'une nouvelle application.

S'agissant des mesures à vous suggérer, je me concentrerai sur la commande publique. Essentielle, elle s'avère en l'état un obstacle au développement de solutions numériques françaises, en particulier dans le domaine de la cybersécurité.

La mise en place d'une certification obligatoire pour les produits achetés en Europe est essentielle. Les raisons en tiennent non seulement aux contraintes du marché local, afin de permettre aux industries européennes de mieux s'exporter, mais aussi à la robustesse même des produits. La récente attaque informatique qui a affecté Microsoft et FireEye en touchant l'un de leurs fournisseurs en supervision, SolarWinds, a montré les conséquences de l'absence de toute exigence de robustesse et de résistance à l'égard de logiciels. En l'occurrence, elle a offert une voie d'entrée béante chez Microsoft, FireEye et les quelque 18 000 autres clients de SolarWinds.

Lors de l'achat d'un véhicule, il semble évident à tout un chacun que les ceintures de sécurité ou le système antiblocage des roues (ABS) fassent l'objet de certifications précises. Il nous faut adopter une attitude semblable au moment d'acquérir un logiciel. Je dirai que nous manquons encore de maturité devant les produits numériques. Le temps viendra où nous porterons comme il se doit toute notre attention à la certification de leur robustesse.

M. Yoann Kassianides. Pour ma part, j'insisterai sur l'importance de bien concevoir, notamment au sein de la représentation nationale, que notre secteur de la confiance numérique se compose d'entreprises de pointe, c'est-à-dire d'entreprises performantes.

Au regard de la commande publique, je préconise avant tout achat effectif de s'enquérir de ses effets du point de vue de la souveraineté. J'abonde dans le sens des propos qui viennent d'être tenus au sujet de la certification. Elle se révèle décisive à double titre.

D'une part, elle permet de vérifier que le service proposé par l'État n'emporte pas de problématique majeure de souveraineté. En substance, il s'agit de s'assurer de la maîtrise des données, de leur stockage d'une manière bien définie et sans possibilité qu'elles servent à d'autres fins que celles attendues.

D'autre part, une certification rigoureuse, au sens où l'entendent l'ANSSI ou l'agence européenne chargée de la sécurité des réseaux et de l'information (*european network and information security agency*, ENISA), garantit la protection du service, ou cybersécurité. Ainsi que le remarquait l'intervenant précédent, elle donne également à nos entreprises, du fait de leur excellence dans ce registre, un avantage certain. Leurs concurrents internationaux s'appuient d'abord sur leur force financière et leur capacité en matière de marketing.

L'exigence de robustesse des produits numériques devrait donc occuper une place centrale. La crise sanitaire actuelle nous en donne une occasion historique.

La demande de numérisation connaît un essor sans précédent. La pandémie a contraint des millions de personnes à recourir au télétravail quand nul n'y était vraiment préparé. Les entreprises ont compris l'importance de la numérisation de leurs activités.

La cybersécurité et la confiance numérique se construisent dès le départ du projet de numérisation ; la souveraineté numérique doit être prise en compte en amont de la commande publique. Il convient des les y intégrer d'emblée au risque de n'y parvenir que beaucoup plus difficilement, voire plus du tout, ultérieurement.

Les enjeux de la souveraineté numérique sont d'ordre stratégique. Ils priment toute autre considération lors de l'acquisition d'un produit informatique. Il importe de définir cette souveraineté comme une priorité nationale, en ne perdant pas de vue qu'elle s'inscrira nécessairement dans un cadre européen. Bien conçus, les outils numériques servent les valeurs fondamentales qui sont celles de l'Europe. Porteur, ce créneau est susceptible d'entraîner l'ensemble du secteur de la confiance numérique dans une dynamique positive.

M. Philippe Latombe, rapporteur. Merci à tous pour ces échanges, le temps que vous nous avez consacré et vos réponses.

La séance est levée à 11 heures.

Membres présents ou excusés

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

Réunion du jeudi 14 janvier 2021 à 9 h 35

Présents. - Mme Virginie Duby-Muller, M. Philippe Latombe, M. Denis Masséglia, Mme Nathalie Serre, M. Jean-Luc Warsmann

Excusés. - Mme Frédérique Dumas, M. Philippe Gosselin