CIO.FOCUS

La souveraineté numérique, un enjeu majeur trop négligé

EN BREF

Eh bien oui, régulièrement, Untel ou Untel va hurler contre les GAFAM, contre les lois extra-territoriales américaines, contre l'impérialisme économique ou encore les abus de positions dominantes. Hurler doit soulager la colère. Mais, ensuite, que faut-il faire ? Il est sans aucun doute plus que temps de se poser cette question. Voici quelques réponses dans ce CIO.focus.

Pour toute demande concernant CIO.focus :
contact-cio@it-news-info.com

Une publication de IT NEWS INFO :
26-28 rue Danielle Casanova 75002 Paris

Rédacteur en chef :
Bertrand Lemaire
blemaire@it-news-info.com
Tél. : 01 41 97 62 10

Principaux associés :
IT Facto et International Data Group Inc.

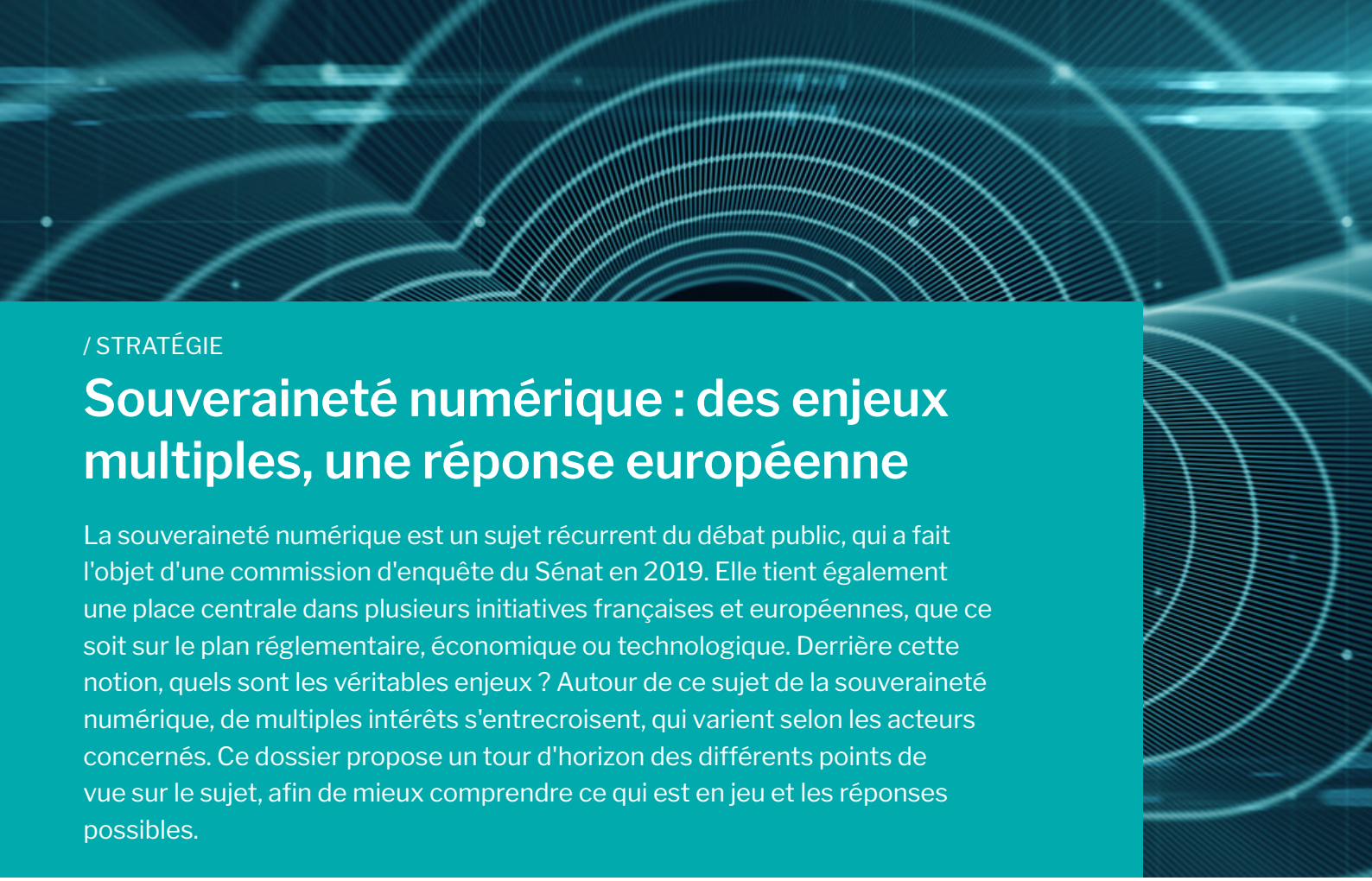
Président et Directeur de publication :
Nicolas Beaumont

Directeur général : Nicolas Beaumont

CIO est édité par **IT NEWS INFO,**
SAS au capital de 3000000 €

Siret : 500034574 00029 RCS Nanterre

SOMMAIRE



/ STRATÉGIE

Souveraineté numérique : des enjeux multiples, une réponse européenne

La souveraineté numérique est un sujet récurrent du débat public, qui a fait l'objet d'une commission d'enquête du Sénat en 2019. Elle tient également une place centrale dans plusieurs initiatives françaises et européennes, que ce soit sur le plan réglementaire, économique ou technologique. Derrière cette notion, quels sont les véritables enjeux ? Autour de ce sujet de la souveraineté numérique, de multiples intérêts s'entrecroisent, qui varient selon les acteurs concernés. Ce dossier propose un tour d'horizon des différents points de vue sur le sujet, afin de mieux comprendre ce qui est en jeu et les réponses possibles.

Depuis une dizaine d'années, la souveraineté numérique revient régulièrement dans le débat public. Toutefois, cette année le sujet a pris de l'ampleur. La pandémie de Covid-19 a en effet contribué à une prise de conscience plus large des enjeux associés. Comme l'observe ainsi le Club Relations fournisseurs du Cigref, « ce n'est plus un sujet réservé aux experts ». La question du traçage des cas contacts Covid-19 a notamment « relancé la question de l'hébergement et de la souveraineté des données dans l'opinion publique. » En 2020, les problématiques auxquelles cherchait à répondre le projet Andromède, cette tentative de cloud souverain français qui s'est soldée par un échec, sont loin d'avoir disparues. Au contraire, la nécessité de protéger les données des citoyens, des États et des entreprises s'est accrue au cours des dernières années, dans un contexte international difficile : l'adoption du Cloud Act en 2018, la crise sanitaire puis économique en 2020 ont mis en lumière certaines vulnérabilités auxquelles il apparaît urgent de remédier. En démontrant l'importance du numérique pour l'activité économique, la crise a aussi souligné la nécessité de préserver un savoir-faire, des ressources et des services associés en Europe, pour ne pas dépendre uniquement des grands fournisseurs américains et chinois. Dans cet environnement géopolitique et économique incertain, comment construire une Europe numérique solide, qui protège les intérêts de ses membres ? Des entreprises privées au secteur public, des fournisseurs de services numériques aux représentants politiques, chacun propose et défend une vision de la souveraineté qui lui est propre. Ce dossier a pour but de présenter les points de vue des différentes parties prenantes et les principaux enjeux du débat.

Du côté du monde politique, le sujet est revenu sur la table en 2019, avec plusieurs travaux concomitants. C'est tout d'abord, le rapport Gauvain sur la souveraineté de la France et de l'Europe, publié le 26 juin 2019, qui pointe notamment le caractère problématique du Cloud Act, promulgué par Donald Trump le 26 mars 2018. « Cette loi fournit la possibilité aux autorités judiciaires américaines d'obtenir des fournisseurs de stockage de données numériques (qui sont tous américains), sur la base d'un simple « warrant » d'un juge américain, toutes les données non personnelles des personnes morales de toute nationalité, quel que soit le lieu où ces données sont hébergées », écrivent ainsi les auteurs du rapport. En avril 2019

est également créée une commission d'enquête sur la souveraineté numérique, à l'initiative du groupe Les Républicains. Présidée par Frank Montaugé, avec Gérard Longuet comme rapporteur, cette commission a présenté le fruit de ses travaux début octobre 2019, sous la forme d'un rapport détaillé. Enfin, Bruno Le Maire, ministre de l'Économie et des Finances, s'est emparé du sujet, auquel il a notamment consacré son discours du 10 septembre 2019 devant le Sénat. « Je considère que notre souveraineté nationale dépend de notre capacité à bâtir notre souveraineté digitale et que la souveraineté européenne dépend aussi désormais directement de notre capacité à construire technologiquement, financièrement, industriellement, notre souveraineté digitale », affirme ainsi le ministre.

L'avenir européen en jeu

Les auditions réalisées dans le cadre de la commission d'enquête ont permis à de nombreux acteurs de faire entendre leur voix sur le sujet de la souveraineté numérique. Le monde académique et professionnel s'est exprimé à plusieurs reprises, notamment à travers l'audition de Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique (ISN). Cet institut créé en 2014 s'est donné pour objectif « de fédérer l'ensemble des acteurs concernés par les mutations numériques de nos sociétés (de l'énergie aux transports, de la maîtrise de l'environnement à la Culture...) et de faire connaître les nouveaux enjeux de la souveraineté numérique auprès des acteurs publics, des acteurs industriels ainsi que des citoyens. » L'ISN compte parmi les membres de son conseil scientifique des entrepreneurs et représentants du secteur numérique français, de nombreux enseignants, des avocats comme Olivier Iteanu, le vice-président de la CNIL Éric Peres ou encore le délégué général du Cigref, Henri D'Agrain. Pour Bernard Benhamou, « le déploiement du numérique n'est pas de même nature que l'électrification ou l'essor de la radio au début du siècle dernier : c'est une transformation intégrale de tous les processus de production. » Il estime en conséquence primordial d'établir un diagnostic lucide, aucun secteur n'étant à l'abri de la numérisation. « Ce qui se joue, c'est l'avenir européen dans son ensemble. Certes, l'État n'a pas encore été ubérisé, mais les plateformes ne demandent pas mieux ! », pointe-t-il. Comme le suggère Bernard Benhamou, la question

« Le déploiement du numérique, c'est une transformation intégrale de tous les processus de production. »

de la souveraineté numérique soulève certains enjeux spécifiques pour l'État et le secteur public. Parmi eux figure bien entendu la cyberdéfense, avec le risque de « conflits hybrides » évoqué par le Général François Lecointre, chef d'État-Major des armées, lors de son audition : des conflits « combinant des attaques sur plusieurs fronts, dans plusieurs champs, dont le champ cyber, et visant aussi la désinformation et la propagande ». La cybersécurité fait également l'objet d'un livre blanc de l'UNION-IHEDN, un groupement d'associations spécialisées qui représentent 10.000 anciens Auditeurs de l'IHEDN (Institut des Hautes Etudes de Défense Nationale) et du CHEAr (Centre des Hautes Etudes de l'Armement). Pour ces derniers, « en matière de numérique comme ailleurs, la souveraineté est la capacité à exercer une autorité et à défendre un espace sur lequel on revendique des droits. Le cyber, quatrième dimension de l'espace national, ne fait pas exception à la règle. » Nadi Bou Hanna, directeur interministériel du numérique, a quant à lui mis l'accent sur les services que l'État offre aux citoyens.


© iStock

« Si l'État n'est pas en mesure de fournir des services de confiance avec le même niveau d'ergonomie et de qualité que ceux des grandes plateformes, la souveraineté numérique en restera au stade de l'ambition. » Celui-ci définit la souveraineté numérique comme « la capacité de l'État à définir sans entrave les bons choix de court, moyen et long terme pour la société et à assurer la réversibilité des orientations [...] À défaut, nous sommes pieds et poings liés, nous restons dépendants. Et la dépendance est le contraire de la souveraineté. » Enfin, la souveraineté numérique au sens démocratique implique également de « garantir les libertés fondamentales des usagers : accès au service public, libre arbitre, intimité numérique... »

Adopter des politiques différenciées

Pour les entreprises françaises et européennes, la souveraineté numérique est un facteur important de compétitivité, comme l'a souligné Christian Nibourel, président du groupement de professions de services et de la commission mutations technologiques et impacts sociaux du Medef, devant la commission d'enquête. Pour celui-ci, la souveraineté numérique se définit en effet comme « la capacité des entreprises à s'adapter et à demeurer maîtresses de leur destin et de leur développement économique et social, tout en respectant les valeurs européennes ». Cela suppose de préserver une capacité à innover, « notamment dans les domaines de la blockchain, de la cybersécurité, de l'intelligence artificielle, de l'ordinateur quantique et du cloud souverain. Nous devons également remporter la bataille des standards et des normes, essentiels en matière de transparence et d'interopérabilité », ajoute Christian Nibourel. De son côté, le Cigref met en avant la nécessité de mieux valoriser les données des entreprises, tout en protégeant ce patrimoine, comme l'explique son vice-président Jean-Christophe Lalanne dans un entretien accordé à CIO.

Les entreprises du numérique sont au premier rang face à ces enjeux. Le secteur était représenté par plusieurs intervenants devant la commission d'enquête. Parmi ceux-ci figurait notamment Loïc Rivière, délégué général de l'association professionnelle Tech in France, qui regroupe plus de 400 éditeurs de logiciels et fournisseurs de services Internet. Parmi eux, une majorité de PME françaises, mais aussi les grands acteurs de la technologie américains. « Dans le domaine numérique, la souveraineté est la capacité de « se gouverner » seul », a rappelé Loïc Rivière en préambule. Il a également souligné que la souveraineté était un objectif, et que chacun (État, entreprise, individu) dépendait des autres pour la mettre en oeuvre, dans une démarche de « gouvernance partagée ». Enfin, il a pointé un certain paradoxe entre le monde numérique,

© fishbones-iStock

« monde de communication, donc d'interdépendance », et l'expression souveraineté numérique. « Dans le cadre d'un État-nation, se gouverner soi-même et décider seul supposeraient d'être strictement et technologiquement indépendant dans tous les domaines : en matière numérique, cela pourrait signifier disposer de notre propre moteur de recherche, réseau social, système d'exploitation ou plateforme de e-commerce. Or l'intérêt de ces outils est précisément d'être adoptés par tous et de communiquer ensemble - c'est d'ailleurs pour cette raison que les gens les choisissent », affirme Loïc Rivière, appelant ensuite à différencier ce qui relève des intérêts vitaux d'un pays (la souveraineté nationale) des problématiques de régulation du marché. Pour celui-ci, « laisser penser que nous pourrions nous doter demain d'un Google français ou d'un système d'exploitation français ne serait pas réaliste par rapport à nos moyens et nous écarterait du sujet. »

Le Cloud Act, un catalyseur

Les grands fournisseurs de cloud américains ont également pris part au débat. Plusieurs de leurs porte-paroles ont ainsi pu s'exprimer lors des auditions de la commission d'enquête, répondant notamment aux préoccupations sur le Cloud Act. Marc Mossé, directeur juridique et affaires publiques de Microsoft Europe, a ainsi considéré que la portée de cette loi était limitée, mettant en avant qu'il s'agissait d'un texte de procédure criminelle. « Il n'autorise pas un accès indéfini et indéterminé à l'ensemble des données, mais uniquement dans le cadre d'une poursuite et d'une infraction, pour des données déterminées qui peuvent effectivement être stockées à l'étranger. » Un avis partagé par Anton'Maria Battesti, responsable des affaires publiques de Facebook France, qui a précisé que cette loi « s'appliquera uniquement sur demandes judiciaires. Il ne s'agit nullement d'une porte dérobée permettant à tout à chacun d'avoir accès aux données. » Ces géants du Web incitent toutefois leurs clients à chiffrer les données sensibles, un degré supplémentaire de protection comme l'explique Stéphan Hadinger, directeur technique d'Amazon Web Services France : « le Cloud Act n'oblige pas les fournisseurs de cloud à déchiffrer les données. Or, comme vous le savez, une donnée chiffrée sans la clé correspondante est complètement inutilisable. »

Certains acteurs du numérique français ont estimé à l'inverse que cette législation représentait un risque bien réel, à l'instar de Michel Paulin, directeur général d'OVH, qui cite le rapport Gauvain. Celui-ci rappelle notamment que dans un contexte de guerre économique, « les données peuvent être utilisées pour

attaquer des concurrents sur le marché. » Pour Michel Paulin, « le Cloud Act est une arme très puissante qui vise directement la souveraineté des États. Son application permet aujourd'hui que certaines entreprises américaines puissent saisir la justice américaine pour qu'elle obtienne ces données. Cette transmission s'opérera sans aucune intervention des juridictions françaises. En ce sens, cela pose un réel problème. » Michel Paulin évoque également le rôle important des États pour soutenir l'écosystème numérique européen. « Nos concurrents bénéficient d'un soutien important de la part de leurs États, qui ont des stratégies en la matière : la Chine a ainsi pour objectif d'être le leader en intelligence artificielle. De même, aux États-Unis, toute la stratégie universitaire de recherche est basée sur un système d'aides, tant privées que publiques. » Il déplore que la France, disposant d'ingénieurs « parmi les meilleurs au monde », voie ces derniers recrutés par les acteurs étrangers du numérique. Enfin, il pointe un enjeu important autour de la maîtrise des données, celui de la réversibilité. « Il est indispensable que les entreprises gardent la possibilité de revenir en arrière si elles le souhaitent », estime-t-il. « Si l'ampleur du coût induit par une telle décision s'avère dissuasive, cette démarche est de fait impossible. Au final, cela alimente la capacité des gros acteurs à préempter les données. »

En se basant sur l'ensemble des auditions, le rapport de la commission d'enquête sur la souveraineté numérique a dressé dans sa première partie une synthèse exhaustive des enjeux évoqués. Rappelant dès le début que le cyberespace fait l'objet d'une compétition intense entre États, il souligne les problématiques liées à la concurrence, avec des entreprises en situation de quasi-monopole dans certains domaines. Le rapport développe ensuite les enjeux d'ordre juridique, en particulier ceux associés aux données : protection des données stratégiques, identité numérique, portabilité et interopérabilité... Enfin, il consacre un chapitre à la question de la souveraineté monétaire, potentiellement menacée par la montée en puissance des cryptomonnaies.

Agir à l'échelon européen

Face à ces multiples problématiques, quelle stratégie adopter ? L'ensemble des acteurs sollicités s'accordent sur certains points, comme la nécessité d'agir à l'échelon européen. Pour le secrétaire d'État chargé de la transition numérique et des communications électroniques, Cédric O, également auditionné, c'est à ce niveau seulement que pourront émerger de futurs champions européens du numérique. « La masse critique nécessaire [...] n'est autre que le marché européen fort de 500 millions de consommateurs ; le marché français ne suffit pas. Nous devons donc définir des règles communes de souveraineté européenne. » C'est aussi à l'échelle européenne qu'il faut penser


© fotostar

les enjeux de maîtrise et de protection des données. Ainsi, pour Bernard Benhamou, « l'un des éléments clés de la souveraineté est la territorialité. » Il estime donc nécessaire de relocaliser les données sensibles en Europe. Un constat partagé par Godefroy de Bentzmann, Président de Syntec Numérique et Pierre-Marie Lehucher, président de Tech in France, pour qui « l'ambition française en matière de souveraineté numérique et de Cloud doit se concrétiser au niveau européen. » Dans un communiqué commun publié en janvier 2020, les deux grandes associations du secteur numérique français (NDLR Celles-ci ont récemment annoncé leur rapprochement) ont formulé dix recommandations pour une ambition européenne en termes de Cloud. La première d'entre elles concerne

> « L'ambition française en matière de souveraineté numérique et de Cloud doit se concrétiser au niveau européen. »

la mise en place d'une politique industrielle à l'échelle européenne, afin de faire émerger des champions du Cloud locaux. « Des offres cloud complètes existent en Europe, l'enjeu est surtout de les aider à gagner en termes de marché pour disposer de champions internationaux. Ce ne sont en effet pas les États qui pourront créer cette offre », soulignent les représentants de l'industrie numérique en France. Ils proposent ensuite différents leviers pour construire et renforcer la souveraineté numérique européenne, à commencer par la maîtrise des infrastructures. En effet, sans datacenters, logiciels, réseaux mobiles et câbles sous-marins reliant les continents, le Cloud n'existerait tout simplement pas : une évidence qu'il est bon de rappeler pour bien comprendre certains enjeux, comme la nécessité de développer et de conserver des compétences techniques de haut niveau. « Quand vos voitures sont guidées par des logiciels étrangers, que vos communications sont transmises par des fibres étrangères, vous n'avez plus votre souveraineté politique », illustre pour sa part Bruno Le Maire dans son discours du 10 septembre 2019.

Un cadre réglementaire harmonisé

Parmi les autres pistes proposées pour bâtir cette souveraineté numérique, le levier réglementaire revient lui aussi régulièrement, de même que la fiscalité. Plusieurs acteurs invitent ainsi à bâtir des règles communes, pour permettre une concurrence équitable au sein du marché européen. Dans leur communiqué, Syntec Numérique et Tech in France recommandent aussi de sécuriser le cadre réglementaire des données. « Toutes les entreprises ont besoin d'un cadre de régulation stable qui ne porte pas atteinte à l'innovation », a affirmé Loïc Rivière lors de son audition. « Il faut aussi que la France s'implique dans la préparation des traités qui concernent le numérique - je pense au Cloud Act ou au projet européen e-evidence - et dans les différents échelons de la gouvernance numérique mondiale. » Christian Nibourel estime également qu'il est primordial de réduire les risques pour les entreprises. « Il y a une déconnexion entre la réglementation française et le Cloud Act. La réponse devra être européenne avec de nouvelles réglementations. » Si le règlement général sur la protection des données (RGPD) mis en place pour protéger la vie privée des citoyens peut selon lui servir d'inspiration, il appelle toutefois à la prudence « sur un futur RGPD des entreprises et sur la mutualisation des données d'entreprises », rappelant que certaines données stratégiques sont le savoir-faire, la propriété de l'entreprise. « Avant de se poser la question de leur mutualisation, il faudrait segmenter les données », pointe Christian Nibourel.


© gorodenkoff-istock

Un troisième volet récurrent concerne le soutien économique et financier au secteur du numérique, en particulier sur les technologies innovantes. Comme évoqué par Bruno Le Maire, « nous avons pris du retard en ne finançant pas suffisamment des technologies de rupture qui sont indispensables pour réussir, notamment dans le domaine de l'intelligence artificielle. » Pour le ministre de l'Économie et des Finances, « l'absence de champion digital en Europe est d'abord liée à l'absence des financements nécessaires pour construire ces champions », ce qui laisse la possibilité aux géants du numérique de racheter les technologies et start-up européennes. Pour y remédier, Syntec Numérique et Tech in France recommandent notamment de mobiliser les acteurs de l'investissement public et privé, mais aussi d'utiliser la commande publique comme levier. Cédric O estime pour sa part que le financement doit d'abord être privé. « Quand on parle de 30 à 40 milliards d'euros par an, aucun État n'est capable de dépenser autant dans une seule technologie. Pour avoir du financement privé, il faut augmenter la part du capital qui va vers les entreprises et attirer les investisseurs privés, notamment étrangers. » Enfin, Christian Nibourel plaide pour « un pilotage de l'innovation de rupture au niveau européen », qui prend en compte la composante temps. « Les innovations vont très vite. Il faut une vision et une permanence dans nos investissements, tout en étant capable de changer de cap rapidement pour pouvoir répondre aux nouvelles innovations. »

> « Quand on parle de 30 à 40 milliards d'euros par an, aucun État n'est capable de dépenser autant dans une seule technologie. »

Préserver les intérêts régaliens

Autre sujet important, celui de la confiance, qui va de pair avec la transparence. Dans son bilan de l'année 2019-2020, le Club Relations fournisseurs du Cigref a ainsi pointé » la dépendance des entreprises américaines aux nuages américains (et de plus en plus chinois). » Pour le Club, « l'enjeu de se doter d'un cloud de confiance, qui respecte les valeurs européennes en matière de transparence et de protection des données, est de taille : les jeux politiques des États commencent à influencer lourdement les choix technologiques de nos entreprises. [...] Les organisations européennes doivent être maîtresses de leur devenir technologique et limiter le risque d'être les jouets de luttes géopolitiques. » Cette confiance passe notamment par l'établissement de normes et de standards pour la sécurité, l'interopérabilité et la portabilité des données, un point évoqué dans les recommandations de Syntec Numérique et Tech in France. Le terme a également été employé par Étienne Gonnu, qui représentait l'association April (défense du logiciel libre) devant la commission d'enquête sur la souveraineté numérique.


© Adobe stock

« La question de la confiance est centrale et doit être soutenue par des garanties juridiques claires. Or, à l'heure actuelle, la confiance dans le secteur informatique est trop souvent déléguée à des tiers. La question est donc de savoir sur quelle base accorder sa confiance. L'un des critères capitaux, selon nous, de cette confiance est la possibilité de vérifier ce qui se cache dans le logiciel... et donc de recourir à un logiciel libre. »

Enfin, certaines recommandations concernent plus spécifiquement le domaine régalien. Loïc Rivière a ainsi insisté sur la mise en place « d'une cyberdéfense européenne », « un axe prioritaire de développement dans lequel nous devons mettre en adéquation les capacités industrielles et nos ambitions de défense. » Il a également pointé la confrontation entre certaines technologies émergentes et le monopole régalien, citant en exemple l'authentification et l'identité numériques, l'essor des cryptomonnaies, les technologies de surveillance numérique ou d'observation par satellite, la cybersécurité, le chiffrement, etc. « En soi, l'innovation est neutre, mais certaines technologies nouvelles pourraient constituer des menaces si le pouvoir régalien ne s'en emparait pas au bon moment et de manière satisfaisante », prévient-il. Si l'État doit se saisir de ces sujets, encire faut-il le faire en respectant l'un des principes phares des services numériques : offrir une expérience utilisateur de haut niveau. Ce point a notamment été évoqué par Cédric O, pour qui le sujet de l'identité numérique est un bon exemple du défi qui est posé à l'État. « Les usages dans le numérique bousculent les pratiques : l'État peut certes développer une carte d'identité numérique mais si elle n'est pas pratique ou aussi simple d'usage que le dispositif d'identité numérique développé par Google ou Facebook, alors les citoyens ne l'utiliseront pas. »

Dans la deuxième partie de son rapport, la commission d'enquête sur la souveraineté numérique a proposé plusieurs grands principes pour guider la stratégie française et européenne en matière de souveraineté, qui rejoignent pour la plupart les recommandations des différentes parties prenantes. Il s'agit tout d'abord de fédérer les acteurs afin d'anticiper les défis. Le rapport réaffirme également de façon claire que la cyberdéfense doit être une priorité. Il invite à favoriser le déploiement des infrastructures numériques sur le territoire français, celles-ci étant aussi un facteur d'attractivité économique. Il encourage également la mise en oeuvre d'une véritable politique industrielle pour soutenir les technologies clefs et sécuriser les technologies utilisées par les secteurs sensibles. Enfin, il met l'accent sur les enjeux de financement de l'innovation, sans oublier la question des talents, un levier lui aussi essentiel.

UN ARTICLE RÉDIGÉ PAR
Aurélie Chandeze, Rédactrice-en-chef adjointe

/ STRATÉGIE

Jean-Christophe Lalanne (Cigref) : « il faut aborder la souveraineté numérique en partant des données »

Le Cigref travaille depuis longtemps sur la question de la souveraineté numérique. Plusieurs de ses membres s'impliquent activement dans l'initiative Gaia-X et dans les travaux de la Commission européenne. Jean-Christophe Lalanne, vice-président du Cigref et également EVP CIO du Groupe Air France-KLM, explique pourquoi ce sujet de la souveraineté est essentiel pour les grandes organisations européennes et détaille les enjeux associés.

Jean-Christophe Lalanne (vice-président du Cigref, EVP CIO d'Air France-KLM) : « quand on parle de souveraineté, on parle avant tout de données. »

Le Cigref est un réseau de grandes entreprises et d'administrations publiques françaises, dont la mission est d'aider ses membres à réussir le numérique. À ce titre, il s'intéresse depuis longtemps à la souveraineté numérique, un sujet stratégique pour beaucoup d'organisations. Pour Jean-Christophe Lalanne, vice-président du Cigref et également EVP CIO du Groupe Air France-KLM, les véritables enjeux ne portent pas sur la construction d'un cloud ou d'infrastructures européennes. Selon lui, si les entreprises se saisissent du sujet, c'est avant tout à travers le prisme de la donnée. « Quand on parle de souveraineté, on parle avant tout de data. C'est de là qu'il faut partir pour comprendre les enjeux. Il faut comprendre quelle est la problématique, ce que l'on cherche à résoudre en termes business, et après seulement on peut aborder le comment. » Pour le vice-président du Cigref, des initiatives comme Gaia-X visent bien davantage à saisir des opportunités qu'à résoudre un problème. « Nous entrons dans l'ère de la data transformation, dans l'économie de la donnée. Nous avons tous à gagner à partager les données, en prenant toutes les précautions nécessaires : par exemple, dans le cadre de la crise sanitaire que nous vivons, le partage des données sur la maladie permet à la recherche et aux médecins de progresser. »

Dans ce contexte, les entreprises prennent conscience de la puissance des données dont elles disposent. « Nous avons des équipements qui regorgent de données. Dans le cas d'Air France KLM, il s'agit par exemple des avions, mais cela peut être des trains, des

installations électriques, des voitures... », observe Jean-Christophe Lalanne. « Ces données, où les mettre ? Comment les gouverner, s'assurer qu'elles ne sont pas soumises à des législations étrangères ? D'un point de vue géopolitique, le monde cyber est fragile. Les données sont un nouveau carburant, facile à piller. Il faut se protéger contre la spoliation et le détournement de nos richesses par d'autres puissances économiques », estime le vice-président du Cigref. La multiplication des données soulève également des enjeux d'ordre environnemental. « Si chacun stocke et traite les données dans son coin, la richesse potentielle est moindre, la quantité de CO^2 générée augmente et les infrastructures ne sont pas rationalisées. Par ailleurs, pour traiter les problématiques liées à l'environnement, il va falloir partager rapidement beaucoup de données », ajoute-t-il.

Une fédération de services et d'infrastructures autour des données

Pour répondre à ces enjeux, à la fois économiques, environnementaux et géopolitiques, le Cigref considère qu'il est souhaitable de mettre en place des services de partage des données mutualisés, le tout à l'échelon européen. C'est guidé par cette conviction que le réseau d'entreprises a rapidement apporté son soutien à l'initiative Gaia-X, lancée en 2019. « Gaia-X n'est pas un cloud européen, contrairement à ce qui a souvent été dit », affirme Jean-Christophe Lalanne. « C'est un ensemble de règles et de principes de gouvernance à mettre en place, avec des espaces par secteur (santé, industrie...). Le but est de construire des plateformes business, qui offrent un ensemble de services autour des données, tout en respectant les règles établies par l'Union européenne, comme le RGPD. Peut-être même que les grands acteurs américains peuvent y apporter leur contribution », ajoute-t-il. (NDLR - les grands fournisseurs de cloud américains et chinois ont en effet récemment rejoint le projet, de même que des éditeurs comme Salesforce.) Pour le secteur du transport aérien, il s'agirait par exemple de mettre des données issues de centaines d'heures de vol à la disposition de différents acteurs, en temps réel et avec toute la sécurité requise, afin de permettre à l'écosystème de proposer des services autour de ces données tout en ne stockant celles-ci qu'une seule fois. Comme le souligne le vice-président du Cigref, « Gaia-X n'est pas une centralisation, mais une fédération d'infrastructures de données. Cela signifie que je peux avoir mes données sur mon cloud privé tout en étant conforme à Gaia-X, afin de les exposer. »

Les 22 organisations fondatrices ont rapidement été rejointes par d'autres, et plusieurs pays sont aujourd'hui représentés. « Il y a des espaces de données à concevoir, avec des sponsors pour chaque domaine », indique Jean-Christophe Lalanne. L'ambition est de taille, mais le programme progresse toutefois à un bon rythme. « Les règles de gouvernance commencent à être établies. Nous allons sans doute voir les premiers Proof of Concept dès 2021 », estime-t-il.

Le Cigref s'est engagé très tôt dans l'initiative, participant aux travaux préparatoires. « Il s'agit de construire des services qui peuvent nous simplifier la vie, autour de la traçabilité, de l'interopérabilité, de la sécurité des données. Gaia-X nous offre la possibilité d'être partie prenante dans la construction de ces standards », apprécie le vice-président de l'association. S'il reconnait que le Cigref s'est montré dubitatif par le passé sur certaines initiatives autour de la souveraineté, il souligne cette fois-ci que les membres du réseau ont « envie d'y croire ». Des organisations comme EDF, Air France-KLM, Safran et Airbus se sont d'ailleurs déjà investies dans le programme. Le fait que le projet soit porté par des acteurs comme Hubert Tardieu, le concepteur de Merise, le soutien apporté par la Commission européenne vont selon Jean-Christophe Lalanne dans la bonne direction. « Les États-Unis, la Chine ont une force de frappe gigantesque à cause de leurs marchés intérieurs. En Europe ce n'est pas le cas. Amazon, Google, Microsoft sont d'abord des entreprises américaines, avec une culture d'hégémonie. La culture européenne est différente, parfois plus fragmentée, mais nous essayons d'aller vers un modèle de fédération. » Un « rassemblement de bonnes volontés » qui a plus de valeur que de rester seuls. « Nous n'avons rien à perdre. Il faut y aller vite, et il faut le faire à un niveau d'abstraction supérieur, qui est celui des données », conclut Jean-Christophe Lalanne.

UN ARTICLE RÉDIGÉ PAR
Aurélie Chandeze, Rédactrice-en-chef adjointe

/ STRATÉGIE

Comment bâtir des clouds souverains

Aujourd'hui, aucun débat sur la souveraineté numérique n'a lieu sans mentionner le cloud. Disposer de services sécurisés, non soumis aux législations étrangères représente en effet un enjeu fort pour les États comme pour les entreprises européennes. Des clouds de l'État à Gaia-X, focus sur les différentes initiatives actuelles et leurs positionnements respectifs.

Bruno Le Maire, dans son discours du 10 septembre 2019, a évoqué la création d'un cloud de confiance français.

La question de la souveraineté numérique occupe de nouveau le débat public, et avec elle l'idée de bâtir un cloud souverain. Toutefois, depuis l'échec du projet Andromède, lancé en 2011, la façon d'aborder cet enjeu a changé. « La dernière expérience menée a laissé un goût amer », a estimé Loïc Rivière, délégué général de l'association professionnelle Tech in France, qui s'est exprimé devant la commission d'enquête sur la souveraineté numérique en 2019. Malgré cela, il a rappelé ensuite qu'il était dans l'intérêt de la France de disposer d'alternatives en matière de cloud. « La question est de savoir où placer le curseur entre un cloud souverain hébergeant uniquement les données sensibles de l'État et un cloud également capable de répondre aux besoins des grands utilisateurs nationaux », affirme-t-il. Afin de ne pas réitérer les mêmes erreurs, Loïc Rivière invite à « bien différencier les données relevant du marché de celles, plus sensibles, entrant dans le champ de la souveraineté numérique. »

Ce constat semble avoir été entendu. Le 27 août 2020, s'exprimant devant les chefs d'entreprise français lors de LaREF, l'événement d'été du Medef, Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance, a opéré cette même distinction. « Nous travaillons sur un cloud souverain pour stocker les données les plus sensibles des entreprises stratégiques pour le pays. Mais l'un des freins concerne la valorisation des données stockées. À l'échelle franco-allemande, nous menons le projet Gaia-X, pour faciliter l'échange et la valorisation des données entre grandes entreprises », a ainsi expliqué le ministre.

De l'État aux entreprises, des exigences différentes

Pour bien comprendre ce qui distingue les différentes initiatives actuelles, il faut d'abord prendre en compte la diversité des besoins et des exigences, y compris au sein d'une même entreprise ou d'un même secteur. Ainsi, pour le secteur public, une circulaire du cabinet du Premier Ministre a précisé le 8 novembre 2018 la doctrine pour l'usage du cloud computing dans l'administration, en proposant un découpage en trois cercles de solutions : le premier est un cloud interne construit par l'État, qui capitalise sur les différents clouds interministériels existants ou en cours de construction. Ce cloud interne est destiné à accueillir des données, traitements et applications sensibles, ainsi qu'à répondre aux besoins régaliens d'infrastructures numériques. Un deuxième niveau de cloud, le cloud dédié, s'appuie sur une infrastructure cloud standard du marché, mais personnalisé pour répondre aux besoins de l'État et reposant sur une infrastructure dédiée. Ce cloud vise notamment à répondre aux enjeux de pérennité des données, dans un modèle de cloud privé. Enfin, le troisième niveau est le cloud externe, un catalogue d'offres porté par les centrales d'achat de l'administration, répondant à un certain nombre de critères minimaux en termes de fonctionnalités, de réversibilité et de sécurité.

Pour les entreprises, l'un des principaux enjeux en matière de souveraineté numérique est de protéger les données sensibles face aux législations étrangères, l'arsenal réglementaire étant une arme de choix pour la guerre économique dans le cyberespace. Cependant, la protection ne doit pas empêcher l'exploitation de ces données. C'est l'équation que cherche à résoudre le programme Gaia-X à l'échelon européenne. À travers Gaia-X, il ne s'agit pas de construire une offre de cloud, mais de fédérer des services existants à travers une série de critères et de standards communs, ainsi que des principes directeurs comme le Security by Design (sécurité dès la conception) et le Privacy by Design (protection de la vie privée dès la conception). Dans Gaia-X, c'est l'utilisateur qui décide où ses données sont stockées, qui peut effectuer des traitements avec celles-ci et pour quels usages, en fonction de sa propre classification. L'objectif est d'accompagner le développement d'un écosystème de confiance autour du cloud, pour permettre l'échange et le partage de données de façon sécurisée, en particulier dans le


© Alvarez-istock

cadre de plateformes et cas d'usages sectoriels. Lancé en 2019 par 22 entreprises françaises et allemandes, le programme a aujourd'hui considérablement grandi, regroupant désormais plus de 300 organisations.

Le cloud distribué, la réponse des fournisseurs de cloud public ?

Si l'approche proposée par Gaia-X permet de répondre à la plupart des problématiques en matière de souveraineté numérique, il est parfois nécessaire d'aller plus loin. C'est le cas notamment pour certains secteurs, notamment les opérateurs à importance vitale, opérateurs de services essentiels ou encore l'administration, qui peuvent nécessiter des garanties supplémentaires pour certains services ou types de données. Pour cette raison, l'État souhaite également développer un cloud de confiance français, qui « doit permettre aux entreprises, privées comme publiques, de stocker leurs données stratégiques en toute indépendance et avec toutes les garanties de sécurité nécessaires », selon Bruno Le Maire. Ce cloud de confiance est mis en place avec des acteurs français du cloud, qui garantissent un hébergement en France. Il passe notamment par la qualification des offres, à travers le référentiel SecNumCloud de l'ANSSI.

Toutes ces approches ont bien entendu des points de convergence, en particulier en ce qui concerne les normes de sécurité et d'interopérabilité. Les différences résident principalement dans le niveau de sensibilité des données concernées et dans les usages envisagés. Enfin, une dernière différence concerne l'implication des fournisseurs de cloud public américains. Plusieurs d'entre eux ont en effet rejoint récemment Gaia-X. Chez ces derniers, il faut également mentionner l'émergence récente d'offres de clouds hybrides (ou clouds distribués selon Gartner), comme Google Anthos, AWS Outposts, Azure Stack ou IBM Satellite. À travers ces dernières, les acteurs américains du cloud proposent de retrouver les mêmes services que sur leurs offres publiques, mais hébergés sur site ou chez un autre partenaire. Une façon de répondre à certains des enjeux en matière de souveraineté, notamment sur la localisation des données, tout en bénéficiant des technologies du cloud public.

UN ARTICLE RÉDIGÉ PAR
Aurélie Chandeze, Rédactrice-en-chef adjointe

© Adobe stock

/ STRATÉGIE

Comment l'Agence du Numérique de Défense va structurer les projets IT des armées

Le nouveau DGNum du Ministère des Armées, Nicolas Fournier, revient sur la création de l'Agence du Numérique de Défense (AND) : sa raison d'être, pourquoi son rattachement à la DGA et ses modalités de fonctionnement aux côtés de la DIRISI, du Comcyber et de la DGNum. Le modèle défendu ici pourrait aussi être pertinent dans les industries privées.

© Ministère des Armées

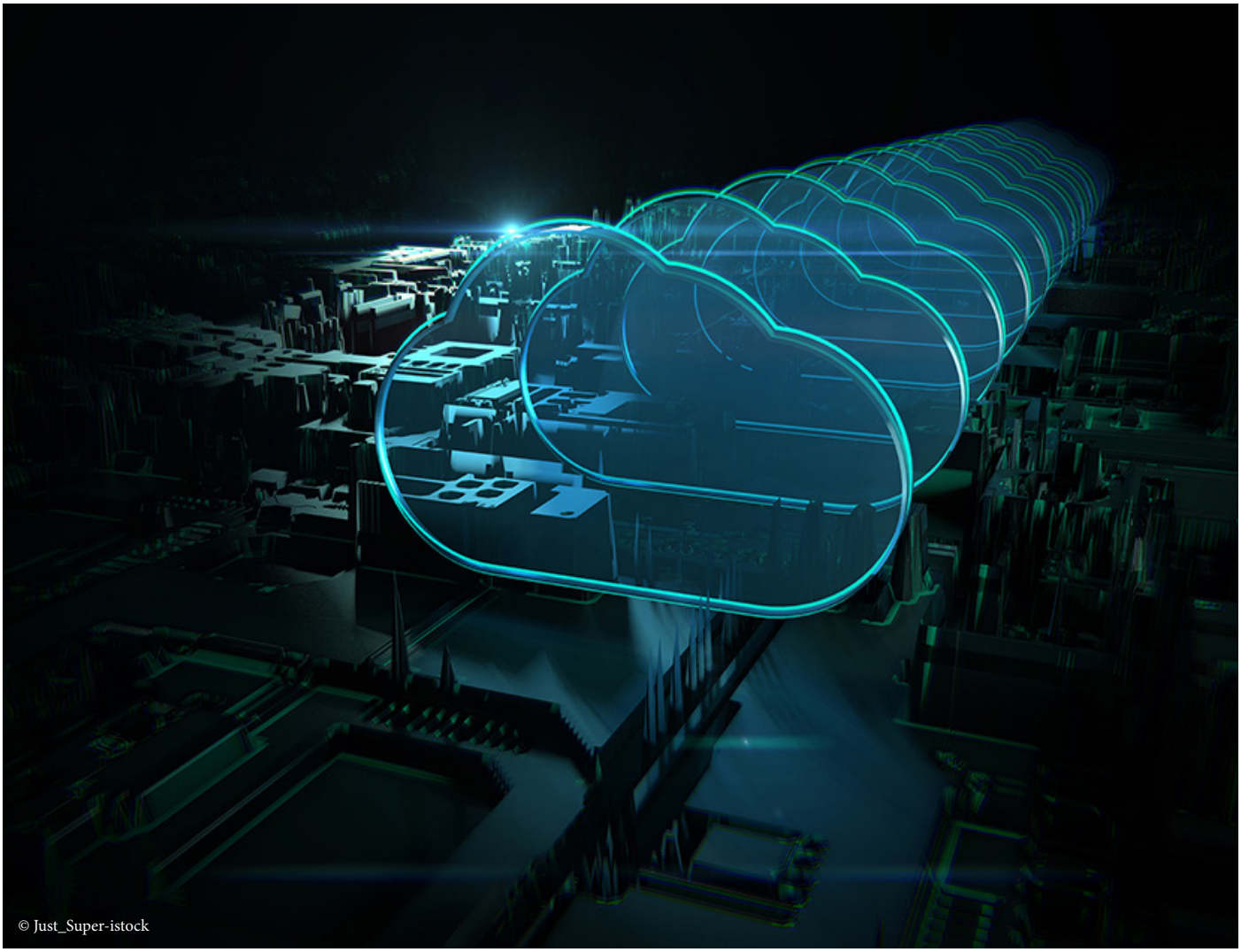
Nicolas Fournier, directeur général du numérique et des systèmes d'information et de communication du Ministère des Armées, a remplacé à ce poste le vice-amiral d'escadre Arnaud Coustillière.

Florence Parly ne cesse pas de se préoccuper du numérique au Ministère des Armées. Mi-2018, un an après sa nomination à son poste actuel, elle avait ainsi transformé la DGSIC (Direction générale des systèmes d'information et de communication) en DGNum (Direction générale du numérique et des systèmes d'information et de communication) avec des compétences élargies. Le 1er décembre, elle a annoncé la création d'une nouvelle structure, l'Agence du Numérique de Défense (AND) pour début 2021. Celle-ci sera le bras armé du Ministère pour mener les projets informatiques, de A à Z.

Cette création ne touche pas aux autres structures déjà en place : la DGNum, bien sûr, mais aussi la DIRISI (Direction Interarmées des Réseaux d'Infrastructure et des SI de la Défense) et le Comcyber (Commandement de la cyberdéfense). Ces deux derniers sont rattachés à l'État Major tandis que la nouvelle AND est sous l'autorité du Délégué général pour l'armement (DGA). La DGNum, quant à elle, est directement rattachée à la ministre. Nicolas Fournier, qui dirige la DGNum, nous a expliqué comment s'articulaient ces différentes structures et les raisons d'être de l'AND.

Quatre structures pour quatre missions bien identifiées

La DGNum est en charge de la gouvernance, de la définition de la stratégie et du pilotage de l'ensemble. Cela ne change pas. De la


© Just_Super-istock

même façon, « il n'est pas question de modifier la DIRISI ou son rattachement » a insisté le DGNum. La DIRISI est en effet l'opérateur ministériel dont « le barycentre reste la conduite des opérations militaires ». Son rattachement à l'Etat-Major est donc conservé et confirmé. Le Comcyber conduit la cyber-défense de l'ensemble du ministère. Sa mission est permanente et consiste à superviser mais aussi à déclencher des actions ou à mener des vérifications. Nicolas Fournier constate : « le seul sujet qui restait était la conduite des projets, ce qui n'est pas le travail de la DIRISI et c'est bien ce sujet qui est traité par la création de l'AND. » On se souvient du traumatisme provoqué par l'échec du programme de refonte de la paye Louvois et les différents audits avaient tous pointé les faiblesses en matière de conduite de projet.

L'AND, donc, va mener les projets, de la gestion de la demande métier à la fin de vie (avec le retrait et la bascule sur le projet de remplacement) en passant par la conception, la réalisation, la mise en production, l'évolution... Elle sera l'interlocuteur unique des métiers et opérera comme une maîtrise d'ouvrage déléguée. Mais le rattachement à la DGA ne peut qu'interroger : le numérique n'est pas (toujours) un système d'arme, dont la conception est l'objet de la DGA. Celle-ci s'occupait évidemment déjà de l'informatique embarquée dans les dits systèmes d'armes (missiles, avions, etc.).

Un pôle unique d'ingénierie

Suite à l'échec de Louvois, c'est en fait déjà la DGA qui avait repris le flambeau pour créer Source Solde, « qui donne satisfaction » précise Nicolas Fournier. Il explique : « ce choix a été fait il y a plus de cinq ans. La première grande raison, c'est que des projets numériques impliquent une conduite de projet complexe et de l'ingénierie. Or, au ministère, le pôle compétent en la matière est bien la DGA : les systèmes d'armes sont confrontés aux mêmes difficultés que les systèmes informatiques, avec des préoccupations similaires de sécurité dès la conception, d'adaptation ergonomique, etc. »

La deuxième raison est relative, justement, aux compétences mobilisées. « Si l'on avait créé un deuxième pôle d'ingénierie, on risquait d'amener des doublons et des dispersions de compétences » pointe le DGNum. Avec l'AND, la DGA se dote d'un pôle original, dédié au numérique, et pas rattaché au pôle opération dont les méthodes sont tout de même différentes. Nicolas Fournier reconnaît tout de même : « certes, les tempos ne sont pas les mêmes. Les systèmes d'armes, très onéreux, sont à stabiliser dès l'origine tandis que, pour le numérique, il est indispensable de disposer d'agilité. Les systèmes d'armes sont livrés et, ensuite, soutenus par les forces ; les systèmes informatiques ont une réalisation qui ne s'arrête jamais, jusqu'à leur retrait. »

L'agilité n'est pas oubliée

L'AND n'est pas créée à partir de rien. Il y a donc, déjà, la fameuse cellule de la DGA ayant mis en oeuvre Source Solde. Mais ce n'est pas tout. L'AND va aussi fédérer des équipes dispersées géographiquement, au plus près des métiers et, le cas échéant, des forces. Nicolas Fournier insiste sur « la nécessité de la proximité géographique avec les métiers ». Ces équipes bénéficieront d'un pilotage matriciel avec, d'un côté, la ligne métier, et, de l'autre, la ligne conduite du projet numérique. L'objectif est d'harmoniser les méthodes en bénéficiant des meilleures pratiques. L'AND sera également à même de mener du conseil de type assistance à maîtrise d'ouvrage pour optimiser la capacité à, à la fois, mettre à jour les systèmes informatiques tout en maintenant à niveau le Legacy. L'équilibre entre l'« ancien » et le « nouveau » sera effectué avec l'éclairage technique de l'AND délivré au métier.

Une telle structuration peut faire craindre que, justement, développement et production soient séparés, en infraction avec les meilleures pratiques de type DevOps. « En fait, l'Unité de Management Socle Numérique créée il y a deux ans et commune à la DGA et à la DIRISI a été la première étape de création de l'AND » rassure Nicolas Fournier. Ce rapprochement est donc maintenu et étendu à tous les applicatifs afin d'assurer, précisément, la cohérence Dev/Ops. Et les services offerts par le « socle » doivent, en plus, progresser au fil des besoins des applicatifs métiers ».

Quels choix de fournisseurs ?

Quand on parle de projets au Ministère de la Défense et de stratégie informatique, on ne peut que s'intéresser aussi aux choix de fournisseurs. Or les contrats avec de grands acteurs américains, notamment Microsoft, interrogent voire inquiètent en raison des propensions de nos amis et alliés d'Outre-Atlantique à une certaine curiosité pas toujours bienvenue quand on parle de la chose militaire. Nicolas Fournier précise de suite : « il y a deux angles dans ce sujet. Le premier est la stratégie de choix des logiciels achetés sur étagère, le second l'aspect contractuel. Sur ce deuxième point, il n'y a pas d'open-bar Microsoft comme on l'a trop souvent dit mais une négociation avec des conditions intéressantes et nous continuons de négocier en acheteurs publics. Sur la stratégie de choix, notre position est constante, avec une logique ouverte, sans réticence à opter pour du Microsoft ou autre chose. »

Il y a cependant une ligne rouge infranchissable : le cloud public. « Certes, la bureautique n'est pas un système souverain mais, par contre, nous devons avoir une garantie absolue d'indépendance et de contrôle de la donnée, donc de souveraineté, et, de ce fait, pour nos produits bureautique Microsoft, le seul cloud possible est le C1 [selon la classification interministérielle] » insiste Nicolas Fournier. Cela dit, le DGNum admet qu'il n'est pas non plus intéressant d'être trop lié à un éditeur ou un autre, ce qui retire dès lors toute capacité de négociation. Nicolas Fournier concède donc : « nous savons qu'il y a des alternatives mais nous avons un raisonnement à la fois économique et sur les compétences des utilisateurs. Aujourd'hui, l'optimum est comme il est. »

UN ARTICLE RÉDIGÉ PAR
Bertrand Lemaire, Rédacteur en chef de CIO