

LE *CLOUD COMPUTING* : DE L'OBJET TECHNIQUE À L'ENJEU GÉOPOLITIQUE. LE CAS DE LA FRANCE

[Clotilde Bômont](#), [Amaël Cattaruzza](#)

La Découverte | « [Hérodote](#) »

2020/2 N° 177-178 | pages 149 à 163

ISSN 0338-487X

ISBN 9782348060250

Article disponible en ligne à l'adresse :

<https://www.cairn.info/revue-herodote-2020-2-page-149.htm>

Distribution électronique Cairn.info pour La Découverte.

© La Découverte. Tous droits réservés pour tous pays.

La reproduction ou représentation de cet article, notamment par photocopie, n'est autorisée que dans les limites des conditions générales d'utilisation du site ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Toute autre reproduction ou représentation, en tout ou partie, sous quelque forme et de quelque manière que ce soit, est interdite sauf accord préalable et écrit de l'éditeur, en dehors des cas prévus par la législation en vigueur en France. Il est précisé que son stockage dans une base de données est également interdit.

Le *cloud computing* : de l'objet technique à l'enjeu géopolitique. Le cas de la France

Clotilde Bômont¹ et Amaël Cattaruzza²

Le *cloud computing* s'est démocratisé au début des années 2000 et s'est rapidement imposé dans l'architecture des systèmes d'information et de communication (SIC) à travers le monde. Alors que la technologie est déjà bien implantée, son marché continue d'augmenter annuellement de 17 % en moyenne³. Cette adoption massive du *cloud* s'explique par l'évolution du contexte technologique. Les volumes de données produites et échangées sur les réseaux nécessitent des capacités de stockage et de traitement toujours plus importantes. Dans le même temps, les SIC se complexifient et leur gestion requiert des compétences de plus en plus pointues. Le *cloud computing* constitue une réponse à ces nouveaux besoins. C'est une technologie de stockage, de traitement et de mutualisation des données numériques qui repose sur l'externalisation de la gestion des ressources informatiques. Le prestataire de services met ses capacités *hardware* et/ou *software* à la disposition de son client qui en a l'usufruit.

Le *cloud*, qui est avant tout un mode d'organisation des systèmes d'information et de communication, est progressivement sorti du champ strictement technique pour s'immiscer dans celui du politique et du stratégique [Cattaruzza, 2019]. Il soulève en effet des enjeux de puissance et de souveraineté qui vont au-delà de questionnements techniques et impliquent *de facto* les acteurs gouvernementaux. Le présent article étudie cette émergence du *cloud* comme objet politique en

1. Doctorante en géographie, université Paris 1 Panthéon-Sorbonne, laboratoire Prodig (UMR8586), membre du centre de recherche Géopolitique de la datashpère (GEODE).

2. Professeur des universités, Institut français de géopolitique, université Paris 8, IFG Lab, centre de recherche GEODE.

3. Moyenne des estimations du cabinet de conseil Gartner sur les cinq dernières années.

France, à travers l'évolution des représentations que les acteurs gouvernementaux français en ont eues au cours de la dernière décennie (2009-2019).

Les représentations sont ici entendues comme « une construction, un ensemble d'idées plus ou moins logiques et cohérentes » dont la fonction est de décrire une partie de la réalité de manière plus ou moins exacte [Lacoste, 1993, p. 1278]. Leur étude révèle la conception que les acteurs ont du *cloud*, mais témoigne aussi de la subjectivité de ces représentations, qui dépendent d'un contexte sociohistorique [Mondada, 2003, p. 190], en l'occurrence des priorités françaises en matière de numérique. Elle montre également l'incidence directe de ces représentations sur l'objet initial [Dubow, 2009, p. 646], et met donc en exergue leur influence sur le développement du *cloud* en France.

Le *cloud* est d'abord apparu dans les représentations comme un secteur d'activité à développer pour la France, afin de disposer en propre de capacités *cloud* qui reposent sur une base industrielle nationale. L'objectif, en premier lieu économique, est de s'émanciper du joug américain, les entreprises étatsuniennes dominant largement le marché, mais aussi de renforcer la puissance française dans un contexte de compétition internationale pour la maîtrise des nouvelles technologies de l'information et de la communication (NTIC). À cette dimension industrielle s'est ensuite ajoutée la question de la sécurité des données. Le *cloud* s'appuie sur des réseaux cybernétiques transnationaux : les données voyagent à travers le globe et la nationalité d'un fournisseur de services peut différer de celle du client final. Cela soulève des inquiétudes quant au respect de la confidentialité, de l'intégrité et de la disponibilité des données. Or les données sont une ressource de grande valeur économique et stratégique, et leur contrôle est aujourd'hui un facteur de puissance. Les États revendiquent donc leur souveraineté *a minima* sur les données relatives à leurs citoyens ou leurs organisations internes. Cependant, l'extraterritorialité des juridictions de certains pays, au premier rang desquels les États-Unis, peut leur refuser cette prérogative en permettant à des États tiers d'accéder à ces données [Bômout, 2018]. Cette préoccupation sécuritaire est un fil rouge dans les représentations des acteurs et devient progressivement un enjeu central.

La construction du *cloud* en tant qu'objet politique ne peut être décorrélée de l'évolution de la réflexion stratégique française sur le numérique qui a lieu parallèlement. Cette réflexion, portée en partie par les acteurs de la Défense, s'est construite autour des menaces et des risques cyber [Desforges, 2018]. Pourtant, ce n'est que tardivement que les risques liés au *cloud* sont énoncés dans les discours politiques, et le *cloud* n'est réellement intégré dans les réflexions stratégiques qu'à partir de 2018. Cela marque, enfin, une prise de conscience quant à l'importance stratégique de cette technologie devenue, pour des raisons d'efficacité, incontournable.

Une préoccupation d'abord économique et industrielle

En France, les premiers plans structurés autour du *cloud computing* s'inscrivent dans une démarche de redressement industriel lancée suite à la crise économique de 2008. Cette crise a révélé les risques systémiques d'une économie mondialisée et a amorcé dans l'Hexagone une réflexion sur la notion de souveraineté économique. L'effondrement généralisé du secteur bancaire induit par la crise des *subprimes* aux États-Unis a effectivement mis en lumière la dépendance économique française, comme celle de la plupart des États dans le monde, au système financier et technologique américain. Ainsi, l'intérêt gouvernemental pour le *cloud* découle d'une préoccupation principalement économique.

Le « cloud souverain » pensé comme une offre technique ex nihilo

L'une des premières apparitions du *cloud* dans les discours politiques français remonte à fin 2009, lorsque le gouvernement constate la montée en puissance des acteurs industriels américains dans ce domaine. François Fillon, alors Premier ministre, explique en janvier 2010 au sujet de l'informatique en nuage : « Force est de constater que les Nord-Américains dominent ce marché, qui constitue pourtant un enjeu absolument majeur pour la compétitivité de nos économies, pour le développement durable et même, j'ose le dire, pour la souveraineté de nos pays⁴. »

C'est donc pour concurrencer les entreprises américaines et développer la croissance industrielle qu'un premier projet de *cloud* national français, dit « *cloud* souverain », est lancé, dans le cadre du programme Investissements d'avenir. Son développement, alors envisagé comme une « centrale numérique de confiance⁵ », est essentiellement perçu comme une opportunité économique et doit conduire à l'émergence d'un acteur industriel français du *cloud*.

Basé sur un partenariat public-privé, le projet bénéficie de fonds gouvernementaux⁶ et doit associer des entreprises françaises. Il est concrétisé en mai 2011, sous le nom d'Andromède, par l'association des entreprises Thalès, Dassault

4. « Discours du Premier ministre François Fillon sur le thème du très haut débit et de l'économie numérique », le 18 janvier 2010 à Vélizy.

5. Assemblée nationale, « Premier ministre, Cabinet de François Fillon, dossiers bureaucratiques de Ferdinand Tomarchio, Conseiller technique pour l'industrie, les services et la compétitivité de février à mai 2012 ». Répertoire numérique détaillé du versement d'archives électroniques 20144725 (20144725/1-20144725/42), Pierrefitte-sur-Seine, 2016.

6. Le *Projet de loi de finances rectificative pour 2010* prévoit ainsi que 1,75 milliard d'euros soit consacré au « développement des usages et contenus innovants, dont notamment le développement de l'informatique en nuage ("cloud computing") ».

Systèmes et Orange. Ces entreprises ont une envergure internationale mais sont encore novices dans le domaine du *cloud*.

En décembre 2011, suite à des désaccords importants avec Orange, Dassault Systèmes quitte Andromède. L'éditeur de logiciels s'associe en février 2012 avec SFR pour proposer une offre concurrente, avant d'annoncer son retrait définitif du projet en avril 2012. S'il est décidé, malgré cela, de poursuivre la démarche gouvernementale de *cloud* souverain, le projet initial Andromède est scindé en deux initiatives distinctes : Cloudwatt et Numergy. Cloudwatt réunit Orange et Thalès, et Numergy est mené par SFR et Bull. En 2015, Orange rachète les parts de l'État ainsi que celles de Thalès et prend le contrôle de Cloudwatt, tandis que Numergy est entièrement racheté par SFR. Ces rachats marquent l'échec du projet gouvernemental.

La mise en place du *cloud* souverain a échoué essentiellement parce que les décideurs politiques avaient une mauvaise compréhension de la technologie. Le fonctionnement technique du *cloud* et la diversité des offres n'ont pas été correctement envisagés, l'environnement industriel a été mal appréhendé et les acteurs privés mal identifiés, et l'objet technique a été pensé indépendamment du contexte économique et social dans lequel il s'inscrit. La demande pour une offre souveraine était alors trop faible, et les instructions étatiques quant à l'utilisation du *cloud computing* par les acteurs publics n'étaient pas suffisamment claires – quand elles n'étaient pas inexistantes. Les potentiels cas d'usage n'ont pas non plus été pleinement considérés et les services proposés se limitaient à de l'hébergement⁷. Par ailleurs, la scission du projet initial a fragilisé les propositions, alors que le marché se répartissait déjà entre les entreprises américaines (Amazon, Microsoft) ultra-compétitives, et les fournisseurs de services *cloud* nationaux (OVH, Gandi, Ikoula...). La volonté étatique de créer de toutes pièces une offre de *cloud* a donc, en sus, été menée au détriment des acteurs déjà implantés. Ainsi, Cloudwatt et Numergy ont manqué de moyens pour se mettre au niveau des autres offres.

Vers une approche inclusive du cloud

Durant la première moitié des années 2010, la crise économique s'éloigne, mais les faiblesses de la base industrielle française dans le domaine du numérique préoccupent le gouvernement. L'économie tertiaire est désormais essentiellement

7. On distingue généralement trois niveaux de service dans le *cloud* qui correspondent à autant de niveaux d'externalisation : le IaaS (Infrastructure as a service), où le prestataire met à la disposition de son client son infrastructure informatique, le PaaS (Platform as a service) où le prestataire fournit également systèmes d'exploitation et logiciels de traitement de bases de données, et le SaaS (Software as a service) auquel on accole parfois le DaaS (Data as a service), où le prestataire gère l'ensemble du dispositif informatique, jusqu'aux applications.

numérique, et son cœur géographique n'est pas en Europe mais aux États-Unis [Bellanger, 2012; Morin-Dessailly, 2013]. Les conséquences de cette dissymétrie globale sont économiques, mais aussi politiques et stratégiques. Elles prennent une nouvelle dimension à l'été 2013, après les révélations d'Edward Snowden concernant la surveillance de masse opérée par la National Security Agency (NSA), rendue possible par le *Patriot Act*⁸.

C'est dans ce contexte qu'en 2013 le gouvernement présente les 34 plans de la Nouvelle France Industrielle. Ce programme, porté par le ministre de l'Économie, du Redressement productif et du Numérique, Arnaud Montebourg, doit permettre d'identifier les priorités de politique industrielle pour la France et les marchés mondiaux particulièrement porteurs⁹. Le *cloud computing* figure parmi les 34 plans. Il fait l'objet d'une dizaine de mesures dont la feuille de route est validée en juin 2014.

Le choix des acteurs industriels impliqués dans le plan *cloud computing* diffère de celui opéré 4 ans plus tôt : le projet est piloté par Octave Klaba, directeur général d'OVH, et par Thierry Breton, PDG d'Atos, deux entreprises reconnues du secteur. Tandis que le gouvernement Fillon souhaitait construire *ex nihilo* un acteur industriel du *cloud*, la démarche de 2013-2014 s'appuie donc, cette fois-ci, sur les compétences d'entreprises spécialistes, elles-mêmes en relation avec d'autres industriels et syndicats professionnels français du secteur (Jolicloud, Cegid, Cozy Cloud...). Ce basculement traduit un premier recul quant aux enseignements à tirer des difficultés rencontrées par Andromède dès 2012. Les acteurs politiques semblent progressivement prendre conscience que le *cloud* est une technologie complexe, maîtrisée seulement par quelques acteurs industriels spécifiques.

Le plan *cloud* prévoit notamment la création d'un label européen de sécurité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), prémices d'une sécurisation de la technologie. Le développement d'infrastructures et d'une fiscalité favorable à l'installation de *datacenters* en France et en Europe est également mis en avant, dans une démarche souveraine en continuité avec le projet Andromède et la vision des gouvernements précédents. La notion de souveraineté reste associée à une perspective économique puisqu'il s'agit selon le ministère, de « renforcer notre souveraineté numérique sur les données personnelles, tout en dynamisant la compétitivité de nos entreprises¹⁰ ».

8. Le *Patriot Act*, formulé au lendemain des attentats du 11 Septembre, impose aux entreprises du numérique américaines de collaborer avec l'administration américaine et de transmettre les données qu'elles hébergent dans le cadre d'affaires touchant à la sécurité nationale.

9. « Nouvelle France Industrielle : 34 plans de reconquête », Le portail de l'Économie, des Finances, de l'Action et des Comptes publics, 12 septembre 2013, consulté le 21 décembre 2019.

10. Ministère de l'Économie, du Redressement productif et du Numérique, « La Nouvelle France Industrielle : présentation des feuilles de route des 34 plans de la Nouvelle France Industrielle », 2013.

La stratégie adoptée est néanmoins peu lisible. L'accent est mis sur la croissance du secteur du *cloud* mais l'absence de projection à long terme doit être notée. Si des mesures concrètes et, pour certaines, majeures sont exposées, le calendrier de la feuille de route ne va pas au-delà de 2015. En outre, le plan *cloud computing* est inséré au milieu d'autres priorités non hiérarchisées, aussi bien numériques qu'écologiques et sociales. Cependant, ce document témoigne d'une approche davantage systémique du *cloud*. Il présente une vision plus inclusive qui commence à placer le *cloud* dans le paysage politique, industriel et social de l'époque.

Une frilosité gouvernementale suite à l'échec du cloud souverain

Cet élan est toutefois freiné par l'échec du projet gouvernemental de *cloud* souverain qui semble avoir entamé l'enthousiasme politique naissant que soulevait l'informatique en nuage. Le gouvernement se détourne un temps de la technologie qu'il n'évoque que frileusement à de rares occasions (figure 1). C'est pourtant à cette période (2014-2018) que les postures stratégiques françaises sur les questions numériques se consolident [Desforges, 2018].

Le *cloud* est, en effet, complètement absent de la *Stratégie numérique du gouvernement* présentée le 18 juin 2015 par le Premier ministre, Manuel Valls¹¹. Cette stratégie se veut un plan d'action pour le numérique français, mais le manque de discrimination et de hiérarchisation des mesures contribue à la production d'un document qui apparaît confus et peu opérationnel¹². Pour appuyer le lancement de la Stratégie numérique du gouvernement français, une consultation nationale, pilotée par le CNNum (Conseil national du numérique) a été menée depuis fin 2014. Le rapport de cette consultation¹³ fait, lui, mention du *cloud* mais essentiellement en traitant d'un usage personnel et individuel de la technologie.

De la même façon, si l'ANSSI évoque le *cloud* dans sa *Stratégie nationale pour la sécurité du numérique* d'octobre 2015, elle ne le fait qu'en référence aux travaux de certification de sécurité pour l'informatique en nuage, communs avec l'Allemagne¹⁴. Il n'est, en outre, fait aucune mention du *cloud* ni dans le *Livre*

11. Premier ministre, *Stratégie numérique du gouvernement*, 18 juin 2015.

12. La stratégie comprend quatre axes, eux-mêmes déclinés en quatorze mesures hétéroclites et dont le niveau stratégique est très variable : il est question de « soutenir la montée en puissance et l'ouverture à l'international de la "French Tech" », comme d'« ouvrir l'«Emploi Store», un bouquet de services pour les demandeurs d'emploi », ou encore d'« accompagner la révolution technologique dans les pays du Sud ».

13. CNNum, « Ambition numérique : pour une politique française et européenne de la transition numérique », rapport remis au Premier ministre le 18 juin 2015.

14. SGDSN, *Stratégie nationale pour la sécurité du numérique*, 16 octobre 2015.

blanc sur la défense et la sécurité nationale de 2013, ni dans la *Revue stratégique de défense et de sécurité nationale* de 2017, alors que les réflexions sur le numérique progressent beaucoup à cette époque dans les cercles Défense.

Le *cloud* est davantage présent dans le programme Industrie du futur, mené par Emmanuel Macron, alors ministre de l'Économie, de l'Industrie et du Numérique. Ce programme, lancé le 18 avril 2015 et présenté en mai 2016, est une actualisation de l'initiative conduite par Arnaud Montebourg et se veut « la matrice de la Nouvelle France Industrielle¹⁵ ». Le *cloud* est principalement abordé sous l'entrée « Économie des données ». En ligne directe avec le plan *cloud computing* de 2013, les projets menés dans ce cadre sont toujours sous la direction de Thierry Breton et d'Octave Klaba, rejoints par Gérard Roucairol, président de Teratec. Le document fait par ailleurs état de l'avancement des travaux depuis la présentation de la première feuille de route : en février 2015, l'ANSSI a lancé le label « Secure Cloud » qui vise à évaluer les garanties de sécurité proposées par un prestataire, et, en juillet 2015, est mis à disposition un guide de bonnes pratiques sur l'utilisation du *cloud* par les collectivités territoriales.

Le programme Industrie du futur s'appuie notamment sur l'étude *Technologies clés 2020*, publiée en mai 2016¹⁶. Cette étude prospective, conduite tous les cinq ans par la Direction générale des entreprises (DGE), cherche à déterminer les technologies stratégiques des cinq à dix années à venir. Le *cloud* est deux fois plus présent dans l'édition de 2015 que dans celle de 2011 (fig. 1). Il est pourtant moins mis en avant dans la version actualisée du programme Nouvelle France Industrielle que dans la version originale où l'informatique en nuage faisait l'objet d'un plan à part entière. Toutefois, il est davantage intégré dans une continuité technologique, amorce d'une vision qui sera développée dans les trois années suivantes. En effet, dans le document de 2016, le *cloud* est à plusieurs reprises présenté en relation avec d'autres technologies émergentes telles que le *big data* et les supercalculateurs.

Désormais une priorité stratégique

À partir de 2018, l'accélération significative des travaux autour du *cloud* témoigne d'évolutions importantes dans les représentations des acteurs politiques. Le gouvernement engage d'ambitieux politiques de transformation numérique

15. Gouvernement français, *Nouvelle France Industrielle : construire l'industrie française du futur*, avril 2016.

16. Ministère de l'Économie, de l'Industrie et du Numérique, *Technologies clés 2020 : préparer l'industrie du futur*, Ivry-sur-Seine, mai 2016.

au sein desquelles le *cloud* occupe une place cruciale. Transparaît une prise de conscience quant à la complexité de l'objet, à son besoin de sécurisation, et à son importance stratégique.

Ces nouvelles représentations découlent en partie de l'évolution du contexte international. Au cours de la seconde moitié des années 2010, les affaires impliquant la manipulation, la divulgation et la confiscation de données numériques se sont multipliées (*Clinton leaks* et *Macron leaks*¹⁷, procès entre Microsoft et le gouvernement américain, cybercriminalité, lutte contre le terrorisme, Cambridge Analytica¹⁸...). Les conséquences politiques et la dimension stratégique des données et des technologies relatives à leur hébergement et leur traitement sont apparues au grand jour.

Un saut conceptuel : une sécuritisation du cloud

Tandis que la sphère politique et publique tente d'appréhender l'informatique en nuage, son adoption par le secteur privé et le grand public se poursuit. Les pratiques évoluent et le *cloud* bénéficie autant qu'il contribue à la servicisation croissante de l'informatique¹⁹ et à la plateformesation de l'économie²⁰. Cette évolution explique en partie le saut conceptuel qui semble avoir eu lieu entre 2015-2016 et 2018. Alors qu'il était encore considéré en 2016 comme une technologie à maîtriser et un signal faible, le *cloud* apparaît soudain en 2018 dans les textes officiels comme déjà bien implanté dans l'environnement numérique quotidien.

C'est sous l'aspect sécuritaire que le *cloud* fait d'abord l'objet d'une attention particulière, au sein de la *Revue stratégique de cyberdéfense* de février 2018 qui

17. Pendant la campagne présidentielle américaine de 2016, plus de 30 000 courriels officiels de la candidate Hillary Clinton datant de la période où celle-ci était secrétaire d'État des États-Unis (2009-2013) sont dévoilés par Wikileaks. Ces courriels avaient été envoyés ou reçus sur la boîte mail privée de la candidate, et non sur celle qui lui était mise à disposition par l'administration. Un cas similaire a eu lieu lors de la campagne électorale française de 2017, alors que près de 20 000 courriels du candidat Emmanuel Macron sont dévoilés à quelques heures du second tour de scrutin.

18. Cambridge Analytica était une société créée en 2013, qui exploitait les données privées des internautes, accessibles en particulier *via* les serveurs de Facebook, pour en tirer des informations et des profilages, qui auraient été vendus à divers clients, dont le candidat Donald Trump, au cours de la campagne américaine de 2016.

19. La servicisation consiste en la location – et non plus l'achat – des capacités numériques.

20. La plateformesation de l'économie, également appelée « ubérisation », correspond à l'utilisation croissante de plateformes numériques permettant la mise en relation directe d'un client et d'un prestataire, quel que soit le domaine d'activité.

lui consacre une section entière²¹. Le document explique la nature juridique, technique, économique, et sociale²² des risques inhérents à l'utilisation de l'informatique en nuage et pointe les dangers pour la souveraineté nationale.

Cette position nouvelle peut être lue comme les débuts d'une sécuritisation du *cloud*, au sens développé par Barry Buzan et Ole Wæver. Selon eux, la qualification d'un problème comme enjeu de sécurité ne dépend pas seulement des risques constatés, mais est aussi un acte de pouvoir permettant aux acteurs politiques de redéfinir les priorités stratégiques et de mobiliser des moyens d'action dont ils ne disposeraient pas autrement [Buzan, Wæver et De Wilde, 1998]. Ainsi, s'il était question en 2010-2014 de « renforcer » la souveraineté nationale, ce sont désormais les menaces portées à la souveraineté qui sont mises en exergue. Plus qu'une opportunité économique et industrielle à saisir, le *cloud* devient une priorité stratégique dans les rapports officiels et les projets politiques. Pour sécuriser la technologie, la *Revue stratégique* insiste sur des solutions telles que le chiffrement, les certifications de l'ANSSI²³, et propose des mesures permettant d'encourager le développement d'une base industrielle nationale et européenne (incitations fiscales, investissements, mise en place d'un cadre de confiance).

Néanmoins, seule une stratégie nationale, harmonisée et commune à toutes les entités de l'État peut permettre d'assurer une sécurité maximale. L'établissement d'une politique étatique globale de recours au *cloud*²⁴ est ainsi préconisé dans la *Revue stratégique de cyberdéfense*.

Ouvrir la boîte noire

Ces recommandations ne tardent pas à être suivies. Le 8 novembre 2018, le cabinet du Premier ministre adresse à tous les services étatiques une circulaire présentant la doctrine d'utilisation de l'informatique en nuage de

21. SGDSN, « Pour l'informatique en nuage, inventer une stratégie de régulation et de protection des données », *Revue stratégique de cyberdéfense*, février 2018, section III.1.4, p. 102.

22. L'aspect social n'est pas développé directement en rapport au *cloud* mais la réflexion, particulièrement développée dans un chapitre sur la dimension humaine du numérique, s'applique également à la technologie.

23. Le label « Secure Cloud », lancé de façon expérimentale en 2015 par l'ANSSI, devient « SecNumCloud » en 2016. Il permet de garantir la conformité d'un prestataire certifié aux exigences de sécurité posées par l'ANSSI. Il comportait à l'origine deux niveaux de certifications, « essentiel » et « avancé », qui seront ensuite réunis en un seul référentiel. SecNumCloud est actualisé en 2018 suite à l'entrée en vigueur du Règlement général sur la protection des données (RGPD).

24. *Ibid.*, p. 141, « Recommandations », entrée « Cloud ».

l'État²⁵. Cette doctrine est le fruit d'une coordination entre diverses agences et services gouvernementaux : sous le pilotage du secrétaire d'État chargé du numérique, elle a été élaborée par l'ANSSI, la DGE, et l'ensemble des directeurs du système d'information (DSI) ministériel au travers de la Direction interministérielle du numérique et du système d'information et de communication (DINSIC)²⁶. Le *cloud* y est présenté comme une « évolution structurelle » des systèmes d'information (SI) qui « permet des gains importants d'efficacité²⁷ ». Dans les représentations, il devient alors un composant essentiel de la transformation numérique de l'État.

L'objectif de la démarche est de « développer massivement l'utilisation de l'informatique en nuage au sein de l'administration et à terme d'en faire la norme²⁸ ». Pour réaliser cette ambition, les spécificités de la technologie et des utilisateurs doivent être prises en compte. Les différents niveaux de service offerts par le *cloud* (IaaS, PaaS, SaaS) et la diversité des usages ne souffrent pas une offre unique, commune à tous les acteurs de l'administration publique. C'est la raison pour laquelle une solution hybride, c'est-à-dire qui mêle *cloud* privé et *cloud* public, est imaginée. Dans le cas d'un *cloud* privé, l'infrastructure est à l'usage exclusif du client. Elle peut être gérée par le client, par un tiers ou par les deux, sur site ou non. Le *cloud* privé garantit la restriction de l'accès aux données grâce à l'isolation de l'infrastructure. Le *cloud* public permet davantage de flexibilité et de facilité d'usage mais son infrastructure, même si elle comporte de solides cloisonnements, est à disposition du grand public et est hébergée dans les locaux du fournisseur de services. Un déploiement hybride conjugue les avantages des deux modèles en permettant d'adapter la solution retenue au type de données hébergées et à leur niveau de sensibilité.

Outre les besoins techniques des utilisateurs, ce sont donc bien, aussi, leurs craintes quant à la sécurité de leurs données qu'il faut entendre. Dans un contexte international où les questions numériques sont une pierre d'achoppement, les acteurs publics, lorsqu'ils sont conscients des risques, ont tendance à privilégier des solutions privées, quitte à renoncer à certains bénéfices du *cloud* public. La politique de migration des SI de l'État dans le *cloud* doit alors inciter les acteurs

25. Cabinet du Premier ministre, *Circulaire du 8 novembre 2018 relative à la doctrine d'utilisation de l'informatique en nuage par l'État*, n° 6049/SG, Paris.

26. Le 25 octobre 2019, la DINSIC devient la DINUM (Direction interministérielle du numérique). Rattachée au service du Premier ministre, la DINUM est sous l'autorité du ministère de l'Action et des Comptes publics. Elle est mise à la disposition du ministre de l'Économie et des Finances et du secrétaire d'État chargé du Numérique, <www.numerique.gouv.fr/dinum/>, consulté le 23 décembre 2019.

27. *Ibid.*

28. *Ibid.*

à choisir les solutions adaptées, qui garantissent un niveau de sécurité suffisant mais n'entravent pas l'innovation.

L'offre proposée aux diverses administrations se décompose donc en trois types de *cloud*, appelés cercles, qui permettent d'héberger des données de sensibilité différente :

- le cercle 1, ou « *cloud* interne » correspond peu ou prou à une solution de *cloud* privé, opérée et hébergée par l'État ;
- le cercle 2, ou « *cloud* dédié » devra s'appuyer sur l'offre standard d'un fournisseur de services *cloud*, opérée sur des infrastructures dédiées ;
- le cercle 3, ou « *cloud* externe » sera constitué d'un catalogue de services et d'applications génériques et sera accessible par le réseau Internet.

Le document produit compte à peine trois pages mais constitue la première stratégie française cohérente en matière de *cloud computing*. La doctrine de 2018 se distingue des réflexions stratégiques antérieures qui ont abordé la technologie comme une boîte noire. Elle s'attelle à détailler l'intégration du *cloud* dans les SIC de l'État et en envisage pleinement la dimension technique. De plus, contrairement au projet Andromède, il s'agit cette fois, en structurant et réunissant les besoins de l'État en matière d'informatique en nuage, de construire la demande et non plus l'offre.

Le cloud de confiance, une urgence stratégique et un argument industriel

Alors que les organismes gouvernementaux mettent en œuvre la stratégie *cloud* de l'État, les inquiétudes face aux risques liés à la nature étrangère des principaux fournisseurs de services et au manque d'alternatives nationales sont toujours autant présentes dans les discours. L'adoption par l'administration Trump en 2018 du *CLOUD Act* (pour *Clarifying Lawful Overseas Use of Data Act*) a ravivé ces craintes. Le *CLOUD Act* contraint effectivement les fournisseurs de services américains, par mandat ou assignation, à fournir aux autorités américaines les données demandées stockées sur leurs serveurs, que ceux-ci soient situés aux États-Unis ou dans des pays étrangers.

En France, le besoin de protéger les données de ce type de loi à dimension extraterritoriale se fait de plus en plus pressant et le concept de « *cloud* de confiance » fait son apparition. Le *cloud* de confiance a d'abord été annoncé en février 2019 par Bruno Le Maire, ministre de l'Économie et des Finances, simplement comme un « *cloud* sécurisé²⁹ ». Il a ensuite été baptisé « *cloud* national

29. Bruno Le Maire, ministre de l'Économie et des Finances, Discours d'inauguration du 8^e *datacenter* d'Equinix, février 2019.

stratégique» deux mois plus tard avant de progressivement prendre son appellation actuelle. Destiné à héberger les données françaises et européennes, ce *cloud* pourra faire l'objet d'un partenariat franco-allemand selon Bruno Le Maire. OVHcloud et Outscale, filiale de Dassault Systèmes, ont été mandatées par le ministre pour formuler des propositions dans ce sens avant la fin 2019.

Le rapport du Sénat sur la souveraineté numérique d'octobre 2019 explique que le *cloud* de confiance permettra de « proposer aux entreprises ainsi qu'à la puissance publique des offres diversifiées, performantes et sécurisées ». Il y est ajouté que, « contrairement au projet de "*cloud* souverain" [...], l'initiative vise, dans un marché qui a aujourd'hui atteint une bonne maturité, à s'appuyer sur des fournisseurs et des offres déjà exposés au marché³⁰ ». Ce dernier point, en affirmant la position des rapporteurs vis-à-vis du *cloud* de confiance, replace la démarche dans la Stratégie *cloud* de l'État de 2018. Il n'est plus besoin de revenir sur les avantages et les risques du *cloud*. C'est maintenant l'encadrement de son déploiement et de son usage qui occupe les esprits.

Le *cloud* est transversal aux problématiques abordées dans le rapport : lois extraterritoriales, attraction des centres de données, mise en place d'une politique industrielle nationale et européenne... L'informatique en nuage est effectivement le socle d'un *continuum* technologique intégrant 5G, Internet des objets (IoT), *big data*, *machine learning*, et intelligence artificielle. Il est donc expliqué dans le rapport que le développement du *cloud* doit être prioritaire sur celui d'autres technologies émergentes : « L'identification et la recherche de la maîtrise de l'ensemble des technologies essentielles pour notre sécurité numérique s'est, à ce stade, pour des raisons de ressources, centrée sur le besoin prioritaire d'un *cloud* de confiance³¹. »

Le développement industriel est autre point important du rapport. La compétitivité de la France pour les solutions d'hébergement (IaaS) est reconnue, mais force est de constater son retard pour les services et applications (SaaS). Les auditions conduites par la commission d'enquête soulignent la difficulté de rivaliser « quantitativement » avec les fournisseurs déjà implantés, mais elles insistent également sur la possibilité de proposer une offre qui se différencierait « qualitativement ». La France et les pays européens pourraient faire de la « confiance » leur fer de lance et cibler un marché qui ne connaît pas, actuellement, d'alternative aux géants américains et asiatiques. Le rapport suggère ainsi de « promouvoir les offres *cloud* européennes se différenciant par leur niveau de confiance³² ».

30. Sénat, *Rapport fait au nom de la commission d'enquête sur la souveraineté numérique*, n° 7, session ordinaire 2019-2020, remis le 1^{er} octobre 2019, p. 144.

31. *Ibid.*, p. 114.

32. *Ibid.*, p. 144.

Conclusion

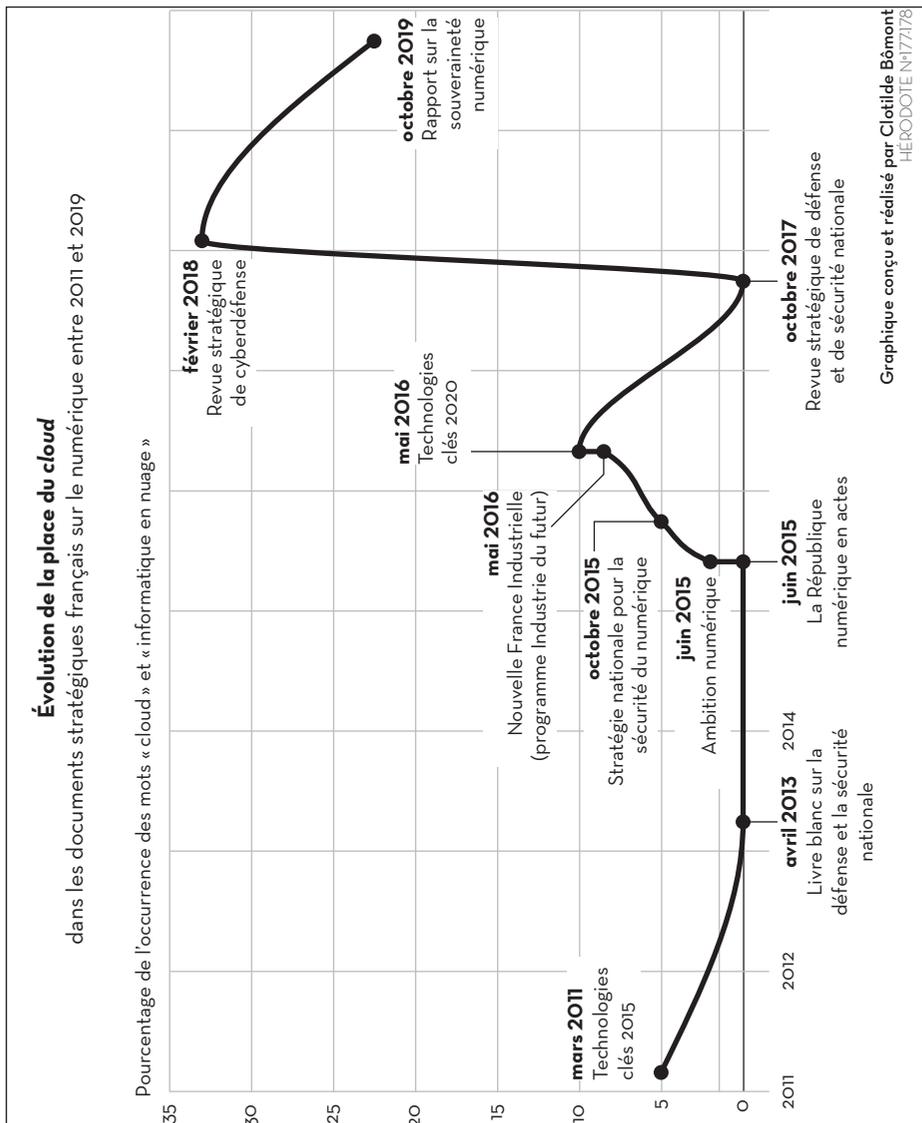
Si la technologie du *cloud computing* est déjà relativement ancienne, nous avons montré ici que la prise de conscience de son caractère stratégique et la mise en place d'une politique cohérente en France sont récentes et sont un processus *en soi* qui nécessite d'être étudié en tant que tel. Nous avons choisi de l'aborder en analysant l'évolution des représentations des acteurs politiques sur la technologie, au travers des textes officiels produits par l'administration entre 2009 et 2019. Ce choix permet de rendre compte des divers positionnements politiques mais limite l'évaluation du rôle d'autres acteurs, en particulier les entreprises privées du numérique, la société civile et l'Union européenne, dans le développement du *cloud* en France. Plusieurs évolutions concomitantes ont néanmoins été mises en lumière.

D'une part, la transcription politique des dimensions techniques du *cloud* a fait l'objet de diverses approches, qui ont progressivement pris en compte la nature complexe et le fonctionnement de cet objet. D'abord abordées dans un effort de labellisation des offres, ses particularités techniques ont finalement été directement intégrées comme les solutions alternatives d'une même stratégie.

D'autre part, l'appréhension des acteurs pertinents pour la mise en place d'une stratégie cohérente s'est affinée. L'implication des partenaires industriels traditionnels de l'État, quand bien même ceux-ci n'étaient pas encore véritablement insérés dans les marchés du *cloud*, a montré ses limites. Aujourd'hui, les acteurs spécialisés sont pleinement intégrés dans la formulation et la mise en œuvre des politiques publiques dans ce domaine.

Enfin, la souveraineté, récurrente à toutes les démarches présentées, admet plusieurs acceptions. Envisagée sous un angle principalement économique en 2009, elle prend un sens davantage sécuritaire dans la seconde moitié des années 2010. Les premières formulations de l'idée d'un *cloud* souverain se référaient à un objet pensé en termes absolus, tant au niveau territorial (infrastructures situées France) que technique (offres françaises). L'approche actuelle est à la fois plus nuancée et plus précise, avec la mise en avant de notions comme l'« autonomie stratégique » et l'adaptabilité des offres techniques (les 3 cercles) en fonction de l'acteur et des données concernées.

FIGURE 1. – ÉVOLUTION DE LA PLACE DU CLOUD
DANS LES DOCUMENTS STRATÉGIQUES FRANÇAIS SUR LE NUMÉRIQUE EN 2011 ET 2019



Hérodote, n° 177-178, La Découverte, 2^e et 3^e trimestres 2020.

Bibliographie

- BELLANGER P. (2012), « De la souveraineté numérique », *Le Débat*, n° 170, p. 149-159.
- BÔMONT C. (2018), « Maîtriser le cloud computing pour assurer sa souveraineté », in TAILLAT S., CATTARUZZA A. et DANET D., *La Cyberdéfense. Politique de l'espace numérique*, Paris, Armand Colin, p. 91-98.
- BUZAN B., WAEVER O. et DE WILDE J. (1998), *Security. A New Framework for Analysis*, Londres, Lynne Rienner Publishers.
- CATTARUZZA A. (2019), *Géopolitique des données numériques. Pouvoir et conflits à l'heure du big data*, Paris, Le Cavalier bleu.
- DESFORGES A. (2018), « Approche géopolitique du cyberspace, enjeux pour la défense et la sécurité nationale. L'exemple de la France », thèse de doctorat, Institut français de géopolitique, Université Paris 8.
- DUBOW J. (2009), s.v., « Representation », in GREGORY D. et al. (dir.), *The Dictionary of Human Geography*, Chichester, Wiley-Blackwell.
- LACOSTE Y. (1993), « Préambule », in LACOSTE Y. (dir.), *Dictionnaire de géopolitique*, Paris, Flammarion.
- MONDADA L. (2003), s.v., « Représentation », in LEVY J. et LUSSAULT M. (dir.), *Dictionnaire de la géographie et de l'espace des sociétés*, Paris, Belin.
- MORIN-DESSAILLY C. (2013), *L'Union européenne, colonie du monde numérique ?*, Rapport d'information du Sénat, fait au nom de la Commission des affaires européennes, n° 443 (2012-2013), 20 mars 2013.
- NYE J. J.-R. (2010), *Cyber Power*, Belfer Center for Sciences and International Affairs, Harvard Kennedy School