MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA RELANCE

Liberté
Égalité
Fraternité

THINK-TANK
DIGITAL
NEW DEAL

LE CLOUD DE CONFIANCE.

Un enjeu d'autonomie stratégique pour l'Europe

Discussions, réflexions et propositions pour un Cloud de confiance,
sous la direction de Laurence Houdeville et Arno Pons.

DGE
DIRECTION GÉNÉRALE
DES ENTREPRISES

Mission Numérique Des Grands Groupes

Avec la participation de

BearingPoint®

Préface de Cédric O

Temporestrum asitatur simil idigeniendel is essit hitia nectur? At voluptas ullorectat reptas solor ad que corepta sperita tatesto deribusam incimus consed quas dit od et veliciis aboresent asperum quae nos expello rporemo eatur? Quia quo odi se si blat ius aliquae volumqu aspit, sum nos esecupta voloreperit as esequi idenis et aut quia ipitiatur si doluptur millestem nonse perchicat quam int ditis iumquis il eaquisqui blam faccuptatus santibus utatem quod quae por susapero dolupta tempore est lique disque culloris estiisin pelibus rehente modit, qui to ipsum exceptatem ident re non nis volecab orecabo. Obitiorrum sit qui reris incimin veliquas nectinvendi illest exceatur?

At ellorro omnimi, et la nonet, volo que simusam quiatecto et idi apici serum rae nonsequis aut eos etum repel modictibus elis quam, quas ditiur? Met, cuptatem faccabo. Namendestium fugit, venihition nus es velique nos et poremquia quuntiuscium rest, issitatem quiant atem ad que reiuria vendi corpor sunt quiaepelici dolecepe omnimen daest, odi sa essequiae. Ut eostiat landipidus mos utam acessit ut ilitas arum ra conectinti dolore, soluptur?

Me dus evel int latisquis maio. Nam fuga. Ita comnihilit officiet aut eos at alitat qui coriae est ped maximi, que modisquod que pratus nem veribus, videst, officienimus ea inctam quam aliquiaturio ditia as eliatur? Atio. Nempost eum que miliqui vendandunt, ant eum ut volorro earit

Assimus dolligenimi, sunt et velestis sae plit quae nonsed ut re nosandae vent

INTRODUCTION

Ce livre blanc, codirigé par la Mission Numérique des Grands Groupes et la Digital New Deal Foundation vient donner la parole à un ensemble de contributeurs, experts du Cloud Computing et penseurs du numérique de confiance.

L'objectif fixé était de faire émerger ; à partir des échanges collectés lors des tables rondes et interviews ; des solutions concrètes économiquement viables, qui permettent d'une part, de soutenir la compétitivité de nos entreprises développeuses de solutions Cloud et d'autre part, de faire connaître ces solutions et d'en favoriser l'adoption par les grands groupes.

La Mission Numérique des Grands Groupes[1] et la Digital New Deal Foundation[2] partagent une même philosophie d'action « saisir, participer à la révolution numérique et non la subir ». C'est dans cet esprit que ce livre blanc a été écrit.

Laurence Houdeville & Arno Pons

1 Voir en annexe la lettre de mission

2 https://www.thedigitalnewdeal.org/en/

MODALITÉS

Animation des GT et rédaction du support : **Laurence Houdeville** (Mission Numérique des Grands Groupes) et **Arno Pons** (Digital New Deal)

Contributeurs : François Desnoyer (Safran Landing Systems Chief Digital & Data Officer représentant de Safran auprès de la Mission Numérique), **Monica Sciortino** (IT manager - Architecture & API Natixis), **Adrien Basdevant** (Avocat, membre du Conseil National du Numérique CNNum), **Adrien Lèbre** (Professeur IMT Atlantique), **Frédéric Desprez** (Director of the INRIA Grenoble-Rhône Alpes research centre INRIA), **Olivier Senot** (Directeur de l'innovation Docaposte, membre fondateur GAIA-X), **Jérôme Martin** (Partner Tec BearingPoint)

Interviews complémentaires : Hubert Tardieu (Président du conseil d'administration de GAIA-X), **Raphaël de Cormis** (VP Thalès Digital Factory), **Patrick Laurens-Fring** (Directeur des Systèmes d'Information – Caisse des Dépôts), **Servane Augier** (VP Développement et Affaires Publiques 3DS OUTSCALE, membre du board de GAIA-X et membre du bureau d'Hexatrust), **Xavier Vaccari** (Chief Strategy Officer – Cloud & AI – Docaposte), **Jean-Noël de Galzain** (Fondateur & CEO – IF Research WALLIX. Président d'Hexatrust), **Marie-Christine Servant** (Responsable unité numérique Société du Grand Paris), **Edouard de Rémur** (Co-fondateur d'Oodrive Technologies, co-pilote du Comité Stratégique de Filière des industries de la Sécurité), Olivier Caleff (expert sécurité et CSIRT), **Olivier Breton** (OVH Sales Director Solutions - Business Unit Commerce EMEA). Sur le sujet « Bâtir et promouvoir une souveraineté numérique nationale et européenne » les députés **Pierre-Alain Raphan**, **Jean-Michel Mis**, **Eric Bothorel**.

Remerciements à **Louis Magnes** et **Prune Zammarchi** pour leur aide dans la production de ce document.

SOMMAIRE

Cadre dans lequel s'inscrit notre publication

Nos travaux s'inscrivent dans le prolongement d'une des propositions du Pacte pour le Numérique : « *Développer des actifs numériques stratégiques pour réduire notre dépendance technologique* »[1]. Aujourd'hui sont identifiées des zones de dépendance dans les domaines de la sécurité ou du Cloud. À court ou moyen terme, d'autres difficultés entrent dans le viseur du Pacte : au niveau des évolutions du matériel (informatique quantique), de la manière dont les infrastructures évoluent (continuum Cloud IoT) et de l'ensemble des logicielles envisagées à court et moyen terme.

Ils s'appuient sur les conclusions du rapport du député de Saône et Loire Raphaël Gauvain[2] qui démontre que « l'abus de lois et mesures à portée extraterritoriale est une menace pour l'ordre économique mondial et un élément de concurrence déloyale, dont il convient de protéger efficacement les entreprises françaises et européennes ».

Ils accompagnent les travaux du Cigref en matière de Cloud de Confiance[3], notamment en participant aux échanges sur GAIA-X et en s'engageant auprès du Comité Stratégique de Filière Industries de sécurité de la DGE dont un des objets est de « développer des solutions de confiance au plan national ou européen sur des domaines clefs, notamment en matière de cybersécurité et de Cloud[4] ».

Ils s'inscrivent dans la suite des actions menées par le SISSE[5]. Cette organisation dédiée à la sécurité économique au sein du ministère de l'Économie et des Finances (MEF) vise à assurer la défense et la promotion des intérêts économiques, industriels et scientifiques de la Nation,

1 *https://pacte-numerique.fr/7-propositions/#6*

2 Rapport Gauvain « *Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale* »

3 *https://www.cigref.fr/cloud-confiance-cigref-travaux-gouvernement*

4 *https://www.conseil-national-industrie.gouv.fr/comites-strategiques-de-filiere/la-filiere-industries-de-securite*

5 *https://sisse.entreprises.gouv.fr/fr/qui-sommes-nous*

constitués notamment des actifs matériels et immatériels stratégiques pour l'économie française ; elle inclut la défense de la souveraineté numérique.

Ils prennent en compte les initiatives variées existantes : des think tanks (T3N sous la conduite de Jacques Attali qui avait présenté, dans un rapport de mai 2017, cinq projets de rupture dont le Cloud européen souverain[6]) et sur un écosystème riche notamment sur les thématiques Data IA : Pack IA (Plan IA 2021 de la région Ile de France[7] avec le Hub France IA[8] et la plateforme TeraLab de l'IMT[9])

Ils s'enrichissent des actions déjà réalisées notamment de l'offre de « Cloud Public » de la DINUM dit « Cercle 3 » Catalogue d'offres Cloud Computing externes génériques accessibles sur internet (notamment en SaaS), porté par des centrales d'achat comme l'Ugap pour en faciliter la commande. Ce troisième cercle, dédié aux applications peu sensibles, promet de «rendre éligible un grand nombre d'offres» pour permettre aux administrations de «bénéficier des meilleures innovations dans le domaine ». Ces offres promettent de faire l'objet d'une labellisation pour veiller à ce qu'elles respectent « des critères minimaux en termes de fonctionnalité, de réversibilité et de sécurité ».[10]

Enfin, au niveau européen, et dans le prolongement des propositions formulées dans le cadre de GAIA-X, le livre blanc suit les directives de l'« *European Data Strategy* »[11] qui vise à faire de l'UE un leader sur le marché de la donnée. La création d'un marché unique des données permettra la libre circulation entre les secteurs et au profit des entreprises, des chercheurs et des administrations publiques.

Les objectifs poursuivis sont de taille :

La Commission européenne a proposé deux initiatives législatives pour mettre à niveau les règles régissant les services numériques dans l'UE : la loi sur les services numériques (DSA) et la loi sur les marchés numériques (DMA)[12]. Le DSA et le DMA ont deux objectifs principaux :

- Créer un espace numérique plus sûr dans lequel les droits fondamentaux de tous les utilisateurs de services numériques sont protégés ;

6 Think Tank Transformation Numérique (T3N) – 10 mesures présidentielles pour une France Européenne leader de la transformation numérique – J. Attali

7 *La Région Île-de-France présente son plan régional sur l'Intelligence artificielle « IA 2021 » et les lauréats du 1er Challenge international « AI Paris Région 2018 »*

8 *https://www.hub-franceia.fr*

9 *https://www.imt.fr/recherche-innovation/recherche/nos-partenariats/teralab/*

10 *https://www.banquedesterritoires.fr/letat-definit-trois-niveaux-de-cloud-pour-concilier-securite-des-donnees-et-acceleration-des-usages*

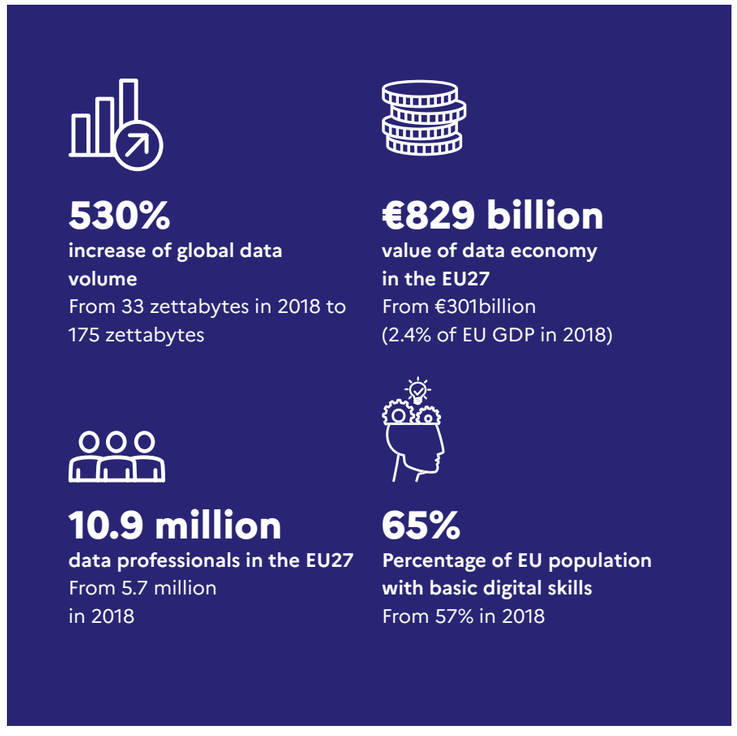
11 *https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en, https://ec.europa.eu/digital-single-market/en/digital-services-act-package*

12 *https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*

- Établir des conditions de concurrence équitables pour favoriser l'innovation, la croissance et la compétitivité, à la fois dans le marché unique européen et au niveau mondial ».

Sans oublier le *Data Governance Act* (DGA) en novembre 2020, qui vise à favoriser la création d'un marché unique européen de la donnée en facilitant notamment le partage de données.

Sur le plan national, le député des Côtes d'Armor Eric Bothorel a réuni autour de lui une mission et produit un rapport[13] avec l'objectif d'entraîner l'Etat vers une véritable « *Politique de la donnée* » à travers un ensemble de réformes d'envergure, afin de se donner les moyens de « *participer aux transformations en cours au niveau européen* ». Ce rapport expose « l'intérêt de l'ouverture de la donnée et des codes source. »



13 *https://www.opendatafrance.net/wp-content/uploads/2020/12/Mission_Bothorel_Rapport.pdf* (décembre 2020)

ÉTUDE PRÉALABLE

En amont de ce livre blanc, une étude quali/quanti a été réalisée à l'automne 2020 auprès d'un panel de 85 Grands groupes Nous présentons ici une sélection de réponses :

Définition du Cloud

"Dans notre entreprise, trois éléments définissent le Cloud :

- Le modèle de service (SaaS, PaaS, IaaS).
- Des propriétés « Cloud » spécifiques (e.g., élasticité).
- Le modèle de déploiement (privé, hybride, public) »

Les cinq qualificatifs du Cloud

« FLEXIBILITÉ, EXTENSIBILITÉ, PORTABILITÉ, MODULARITÉ, ÉLASTICITÉ »

CHIFFRES CLÉS

50%

des entreprises interrogées sont prêtes à adopter une architecture distribuée ouverte (Edge Computing) pour les raisons suivantes :

- « sécurisation des systèmes d'information (Firewalling et gestion d'identités) » ;
- « Pour des raisons de latence et de résilience (Cloud + réseau) et de cyber-protection » ;
- « Dans notre entreprise on définit le « Edge Computing » comme un modèle consistant à déporter le processing (et potentiellement le stockage / staging) au plus près de utilisateurs finaux ».

75%

des entreprises interrogées pensent que le Cloud Act et le Patriot Act font courir un risque à la sécurité des données.

90%

considèrent qu'il y a un risque de perte de souveraineté économique pour l'Europe dans la montée des Cloud américains ou chinois.

Les raisons qui poussent au choix de Cloud non européens :

« Pour l'instant les acteurs du marché les plus avancés en termes d'innovation sont non européens malheureusement...Les évolutions concernant le Privacy Shield vont peut-être «forcer» les acteurs à mieux encadrer les sujets de protection de données »

« e-time to market : l'existence de nombreux services fait gagner un temps précieux pour mettre sur le marché des solutions et services numériques.
C'est un compromis risque / bénéfice qui donne le résultat de cette décision ».

Services prioritairement attendus de la part d'un Cloud européen :

« En dehors des offres IaaS existantes à date, Via OVH Cloud par exemple :

- Data : des services de stockage et d'analyse de la donnée à l'échelle, performants et efficients (type Google Big Query) et des services d'IA type AWS SageMaker ou GoogleIA Platform)
- Bureautique collaborative : concurrents GDPR compliant à G-Suite ou Office 365.
- Suite e-commerce packagée type SalesForce Commerce Cloud ou Shopify
- Suite CRM, marketing, ads et media concurrentes de celles de Google, d'Adobe ou de SalesForce qui sont omniprésentes.
- Services SaaS, PaaS spécifiques pour des usages retail (e.g., moteur de recherche produits, applicatifs digitals en magasin, optimisation des stocks)
- Offres liées à l'ingénierie logicielle type automatisation CI/CD
- La gestion des identités »

« Des data centers avec la conservation des données strictement en Europe. Un backup de continuité de service européen en cas de clash géopolitique avec des pays hors Europe »

« ID as a service (IDaaS) avec AuthO par exemple / IAM - VM Linux / Blob storage compatible S3 / Key secret management system / HSM on demand / Application gateway : load balancer, waf, traffic management / Virtual network management / Ingress/Egress filtering / Cloud SIEM / API devOps / CI/CD Git Repository »

« Kubernetes as a service, architecture micro services, chiffrement avancé »

« Hébergement des données en Europe, développement avec un customer council, des partenariats avec des réseaux universitaires européens et des certifications »

Démarches à entreprendre pour dépasser la mainmise des hyperscalers actuels (investissement public, lois, création de datacenters dans tous les pays …)

« Investissements intelligents dans la création de services à valeur ajoutée dans les pays Européens

- Pour cela, faire le recueil de besoin d'un nombre large d'utilisateurs (établissements publiques et compagnies multi-secteur).
- S'appuyer sur des acteurs européens innovateurs (type OVHCloud, CleverCloud…) montrant un devoir d'exemple étatique et étant prudent sur une éventuelle entrée des Cloud providers US / Asie dans GAIA-X.
- Poursuivre l'encadrement légal de l'usage de données autour de la GDPR, à des niveaux équivalents aux lois américaines ou asiatiques (qui interdisent par exemple l'export ou le traitement de données du territoire) ».

« Il faut nécessairement un arsenal juridique plus important. Le Digital Services Act va dans ce sens. Les crédits sont également importants, mais ne pourront être apportés exclusivement par des fonds publics => une forme de mutualisation des investissements entre industriels devra permettre de faire émerger des standards ».

Cas d'usages sur lesquels les entreprises souhaiteraient travailler (exemples cités) :

« Le sujet de l'hébergement des données de sécurité (SIEM) pourrait constituer un cas d'usage pour un Cloud souverain »

« Auditabilité des traitements automatisés des données »

Dans le cadre d'une verticale commerce :

« Nous avons une multitude de use cases liés à l'e-commerce, le digital en magasin, la logistique, la gestion des marchandises ou encore la traçabilité alimentaire »

Utilisateurs de solutions des fournisseurs de Cloud Européens ? (Orange, OVHCloud, Scaleway (Illiad), Atos, Docaposte, Outscale)

35% des entreprises consultées sont utilisatrices de solutions des fournisseurs de Cloud européens (Orange, OVHcloud, Scaleway (Illiad), Atos, Docaposte, Outscale)

15% des entreprises utilisatrices de solutions de fournisseurs de Cloud européens ont choisi OVH Cloud

MIEUX DÉFINIR LA SOUVERAINETÉ : UN ENJEU DE CLARIFICATION

Des échanges avec les participants est née la conviction que nous devions, en introduction, définir la souveraineté. Très vite, la question de l'autonomie en matière de choix de gouvernance et choix d'approvisionnement est apparue comme centrale. C'est cette préoccupation qui a guidé notre analyse de la souveraineté. Pour autant, l'utilisation d'un tel concept appliqué au numérique porte en elle un certain nombre de défis : en effet, de quelle manière la souveraineté, fondée sur le territoire physique, peut-elle s'appliquer au numérique et spécifiquement au Cloud ? Comment, dans un marché dominé par les géants du numérique, faire advenir différentes formes d'autonomie dans le marché du Cloud ? Enfin, comment faire pour que ce critère d'autonomie constitue le socle d'un Cloud de confiance ?

SOUVERAINETÉ

La souveraineté numérique, un concept géopolitique

Les activités humaines, qu'elles s'exercent dans les sphères personnelle ou professionnelle, sont aujourd'hui largement organisées par la technologie et les outils numériques. De cette organisation nouvelle des sociétés a émergé un rapport de force public-privé, opposant les États et les grandes entreprises qui dominent les réseaux numériques. Dans le même temps, la maîtrise des technologies numériques constitue un terrain d'affrontement nouveau entre les grandes puissances internationales, au premier rang desquelles les États-Unis, la Chine et l'Europe.

Apparu dans les années 2000, notamment popularisé par Pierre Bellanger dans son ouvrage du même nom, le concept de *souveraineté numérique* a pris une place prépondérante dans le débat public. Si la menace semble identifiée, il n'existe pour autant pas de consensus quant à une définition juridique commune de ce concept. Certains l'emploient, d'une part, pour évoquer « *un objectif d'autonomie dans des choix d'outils, d'infrastructures ou de technologies de l'information* », quand d'autres l'utilisent, d'autre part, pour décrire « une forme de protectionnisme qui serait un peu déguisé » Adrien Basdevant - Basdevant Avocats, CNNum. A la pluralité de définitions de la souveraineté numérique s'ajoute – ou plutôt se déplore – l'inexistence d'une acception juridique du terme *souveraineté numérique* ; peut-être émergera-t-elle demain ? Sans définition juridique précise, cette notion reste finalement dépendante des interprétations qui en sont faites.

> **"La souveraineté est un concept géopolitique lié au contrôle et à la façon dont on l'exerce sur un territoire"**
>
> Adrien Basdevant - Basdevant Avocats, CNNum.

Depuis sa définition originelle par Jean Bodin au XVI[ème] siècle, la définition de la souveraineté s'est stabilisée trois siècles plus tard par le juriste français Louis le Fur, qui fait de la souveraineté la qualité d'un État « *de n'être obligé ou déterminé que par sa propre volonté, dans les limites du principe supérieur du droit, et conformément au but collectif qu'il est appelé à réaliser.* »

Or en juin 2013, Edward Snowden révèle au Guardian et au Washington Post l'ampleur des écoutes téléphoniques et de la surveillance numérique menées par ses employeurs de l'époque, la NSA et la CIA. Une série d'accusations s'élève contre les gouvernements américain et britannique, accusés d'avoir mis sur écoute certains dirigeants européens, notamment Angela Merkel[14]. Cette atteinte grave à la souveraineté des États se double

14 https://www.rts.ch/decouverte/sciences-et-environnement/technologies/protection-des-donnees/6199557-affaire-snowden-rappel-des-faits.html https://www.lemonde.fr/pixels/article/2019/09/13/ce-que-les-revelations-snowden-ont-change-depuis-2013_5509864_4408996.html

d'une atteinte non moins grave à l'indépendance des alliés des USA, et interroge profondément la manière dont les États-Unis considèrent leurs « alliés », pris de facto dans une relation de vassalité. La prise de conscience de ces pratiques de surveillance des agences gouvernementales américaines et britannique (permises par le Patriot Act à la suite du 11 septembre 2001) vient clore un cycle de confiance dans le partenariat transatlantique construit depuis 1945. Le retentissement médiatique mondial des révélations d'Edward Snowden a ainsi durablement ébréché la confiance des européens vis-à-vis des alliés américains, et ce faisant a démontré pour les dirigeants de l'Union la nécessité de protéger nos données.

Depuis, l'Europe commence à se positionner sur son indépendance, et déclare vouloir s'affirmer non seulement pour celle-ci, mais aussi comme troisième voie, porteuse de ses propres valeurs, entre les États-Unis et la Chine[15].

15 Europe's third way.

Le terrain de jeu de la souveraineté numérique et la nécessité de sortir d'une relation de dépendance

L'expression de la souveraineté numérique, ou plutôt son exercice, peut se jouer à plusieurs niveaux distincts, selon que l'on se réfère à un Etat, à une entreprise ou à un individu :

- Au niveau des États, désireux de prolonger leur pouvoir de réglementation, voire de coercition, sur les réseaux numériques. C'est le cas du Cloud Act.

CLOUD ACT :
« CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT »

Est une loi fédérale américaine promulguée le 23 mars 2018. Elle modifie le chapitre 121 du Titre 18 du *United States Code*, dénommé *Stored Communications Act* (SCA) de 1986 en autorisant les instances de justices judiciaires ou administratives (fédérales ou locales) d'obtenir des opérateurs télécoms et des fournisseurs de services de Cloud Computing établis sur le territoire américain, des informations stockées sur leurs serveurs qu'ils soient basés aux États-Unis ou dans des pays étrangers.

- Au niveau des entreprises : grâce à leur pouvoir de marché et leur hégémonie globale, un certain nombre de multinationales dessinent les règles de l'espace numérique et notamment celles d'internet posant par là même la question de leur légitimité démocratique à modérer le débat public.

TRUMP BANNI DE TWITTER

La décision de Twitter de supprimer le compte du président américain Donald Trump – encore en fonction au moment des faits – constitue une preuve de cette hégémonie. En d'autres termes, une entreprise privée, par cette décision, s'est imposée comme le régulateur mondial de la liberté d'expression, alors même que les bornes de celle-ci diffèrent d'un pays à un autre. De même, en faisant valoir ainsi ses conditions générales d'utilisation (CGU) sur le représentant élu d'une nation souveraine, l'entreprise Twitter a de fait imposé sa régulation privée sur une situation politique chaotique et floue (l'attaque du Capitole le 6 janvier 2021), prenant de court le législateur américain et laissant l'utilisateur Trump sans recours possible. Cette absence de recours systématique atteint son plus haut degré de problématicité avec ce cas, illustrant l'intersection des droits de l'usager et du citoyen. Comment dès lors concilier l'impératif de contrôle effectif des données de la part des entreprises avec la nécessité pour toutes les parties prenantes d'en encadrer la pratique ?

- Au niveau des citoyens et des collectifs d'individus : Alors que la capacité des utilisateurs à s'autodéterminer et à choisir librement dans le cyberespace s'amenuise, les citoyens revendiquent, par exemple, un contrôle et une maîtrise plus efficace de leurs données personnelles.

La notion de « dépendance » s'articule à tous les niveaux d'expression de la souveraineté, prouvant que le numérique est finalement devenu, au fil du temps, un sujet politique. Cette dépendance peut être technologique ou juridique, et à chaque fois, elle met en lumière une absence d'alternatives.

Dans une tribune, le député de la Loire, Jean-Michel Mis, rappelle à ce propos « *Par ailleurs, la Commission européenne dans un document de réflexion publié le 10 mai 2017*[16]*, avait déjà évoqué la mise en place de « nouvelles règles destinées à créer des conditions de concurrence équitables*[17] *», et de « mise en place d'instruments de défense commerciale efficaces* ».
Le 19 février 2020, elle insistait : « *L'Europe doit reprendre possession de ses données. Le règlement général sur la protection des données a été un premier outil indispensable, mais il nous faut aller beaucoup plus loin. Les données produites en Europe doivent rester en Europe* ».

16 Document de réflexion sur la maîtrise de la mondialisation, Commission européenne, 2017-0510.
17 *https://www.jeanmichelmis.fr/reflechir-ensemble-a-une-nouvelle-grammaire-du-numerique-pour-la-france/*

> « Dans l'exemple de Twitter, la problématique n'est pas tant de savoir si un acteur privé peut faire appliquer ses propres conditions générales d'utilisation ou de savoir si ces conditions générales d'utilisation sont plus ou moins importantes que la Constitution mais c'est de savoir si les utilisateurs bénéficient de mécanismes de recours pour contester les décisions prises par des plateformes, et surtout si ces utilisateurs bénéficient d'alternatives équivalentes en matière de services"
>
> Adrien Basdevant - Basdevant Avocats, CNNum.

Le Conseil de l'Europe, dans ses conclusions sur l'importance de la technologie de la 5G[18], a rappelé lui aussi que « *les réseaux 5G prendront place parmi les infrastructures essentielles pour le maintien de fonctions sociétales et économiques vitales. L'approche de la sécurité des réseaux 5G doit être globale et fondée sur les risques. La sécurité de la 5G est considérée comme un processus continu, qui commence avec le choix des fournisseurs puis se poursuit tout au long de la production des éléments du réseau et durant toute la durée d'exploitation des réseaux* ».

L'émergence de la prochaine génération de technologie mobile, la sixième (6G), devra également se poser en termes de souveraineté. Alors que la Chine, la Corée du Sud et les États-Unis ont été les premières puissances à se lancer dans la 5G, la France et l'Europe doivent envisager la 6G en termes de dépendance / d'indépendance technologique.

En parallèle de la dépendance technologique, il existe une forme d'assujettissement juridique. Depuis quelques années, les enjeux liés à l'application extraterritoriale de législations de pays tiers ont souvent animé les débats, voire orienté des décisions stratégiques publiques ou privées. Le *Cloud Act*[19] (voir encadré) autorise par exemple les autorités américaines, en cas de suspicion de crime ou de menace terroriste, à accéder aux données stockées par des opérateurs américains quelle que soit leur localisation dans le monde. A bien des égards, le *Cloud Act*, *nous l'avons vu,* constitue une illustration probante de la dépendance juridique des États et des entreprises françaises et européennes vis-à-vis de la puissance américaine et sa législation. Néanmoins, les puissances étrangères peuvent avoir recours à d'autres instruments afin d'accentuer notre dépendance, comme par exemple les interdictions commerciales en Chine ou les demandes de licences d'exportation.

Un autre exemple est celui du « *[…] projet chinois de la Belt & road initiative (BRI) vise quant à lui à atteindre le marché européen à l'aide d'infrastructures non seulement ferroviaires et portuaires, mais aussi numériques, conduisant les grandes plateformes chinoises à investir de manière croissante dans des data centers situés sur le territoire européen : les enjeux géopolitiques et de sécurité liés à la gestion des données ne sont plus seulement transatlantiques mais de plus en plus eurasiatiques* » Rapport Thieulin CESE

Cette sujétion européenne renvoie finalement à un monde où des conditions générales d'utilisation s'imposent à nos constitutions et nos règles. Notre état de dépendance, technologique, juridique ou autre, met surtout en lumière une absence d'alternatives crédibles, comme si nous nous avouions perdants dans la bataille du réseau et des infrastructures de calcul (i.e. centrales numériques).

DE LA 5G À LA 6G

La 5G est le premier pas vers la généralisation de l'internet des objets (IoT). Elle se différencie de la 4G que nous connaissons non seulement par la vitesse de transmission des données, mais surtout par sa capacité à permettre de nouvelles utilisations de l'IoT grâce à des performances améliorées. Par exemple, la réduction de la latence pour les services utilisant le Cloud est indispensable pour les voitures autonomes. La 5G permettra aussi de réduire la consommation électrique des objets connectés, leur permettant ainsi de fonctionner des mois voire des années sans assistance humaine. Pour autant, les risques en termes de sécurité sont réels, que ce soit en termes de menaces internes ou de menaces externes. En interne, le problème du stockage de données par les opérateurs 5G se pose. Sur le plan des menaces externes, la démultiplication des nouveaux usages, logiciels et objets augmente la surface d'attaque du réseau. Ainsi, chaque nouvel usage créé par la 5G doit être pensé par ses concepteurs comme une faille de sécurité potentielle à résoudre.

La 6G est un sujet qui émerge peu à peu, mais qui reste à un développement embryonnaire. Ses usages potentiels ne sont pas encore tous identifiés, mais certains opérateurs de la filière télécoms publient les premiers livres blancs. D'après Business Korea, le gouvernement sud-coréen (pour l'instant le plus investi dans la 6G) aurait sélectionné cinq axes de projets expérimentaux : « la santé, les contenus immersifs (réunions holographiques à distance en temps réel et non en présentiel), les voitures autonomes, les villes connectées et l'industrie ». Les projets semblent pour l'instant tournés vers un usage industriel plutôt que grand public, comme l'usage des essaims de robots et des capteurs intelligents pour les domaines de l'hôtellerie, les hôpitaux, les entrepôts et la livraison.

Sources :
https://www.arcep.fr/la-regulation/grands-dossiers-reseaux-mobiles/la-5g.html
https://www.thalesgroup.com/fr/europe/france/dis/mobile/inspiration/5g
https://www.journaldunet.com/solutions/dsi/1440542-les-enjeux-de-cybersecurite-de-la-5g/

18 Conseil de l'Europe, 2019-12-03, Communiqué de presse sur l 'importance de la technologie 5G et risques pour la sécurité – le Conseil adopte des conclusions.

19 Clarifying Lawful Overseas Use of Data Act en anglais https://www.justice.gov/opa/press-release/file/1153446/download

Le champ d'application géographique de la souveraineté numérique

Si l'on s'intéresse à son origine et à sa sémantique, la notion de souveraineté correspond à « *l'exercice du pouvoir sur une zone géographique et sur la population qui l'occupe* »[20]. Or l'abolition des frontières physiques permise par le numérique pose la question du champ d'application géographique de ce concept : doit-il se penser à l'échelle nationale, à l'échelle transnationale dans le cadre de l'Union européenne, ou à l'échelle internationale ? Blandine Eggricks, directrice des relations institutionnelles de La Poste rappelle à cet égard, que « *le sujet de la fiscalité numérique, prépondérant dans le débat public depuis quelques années, constitue un exemple pertinent. Aujourd'hui, les règles internationales en matière d'impôts sur les sociétés ne sont plus adaptées aux réalités de l'économie numérique et n'englobent pas les modèles d'entreprises pouvant dégager des bénéfices à partir de services numériques dans un pays sans y être présent physiquement. Face à cette problématique, une réponse internationale ou a minima européenne doit être trouvée. Néanmoins, alors même que l'impôt est considéré comme un instrument essentiel de la souveraineté d'un Etat, la règle de l'unanimité sur les questions fiscales au niveau européen rend difficile – voire impossible ? – l'éclosion d'un consensus en raison des choix politiques et économiques de chacun des États membres* ». Plus largement, cela prouve que l'Union européenne ne s'est pas encore dotée d'une capacité autonome de décision afin d'exercer collectivement sa souveraineté.

L'autonomie stratégique fait partie d'une vision française qui tente de s'imposer en Europe, notamment contre l'Allemagne (qui y vient progressivement) et les autres pays dépendants de l'OTAN pour leur sécurité. Cet enjeu est devenu un sujet européen «grâce» à l'ère Trump et son anti-multilatéralisme qui a inquiété ses partenaires trop dépendants des États-Unis. On peut comprendre l'autonomie stratégique comme une volonté d'affranchissement de notre dépendance vis-à-vis d'une puissance extérieure, même amicale. C'est une vision assez Gaullienne de la géopolitique selon laquelle l'alliance n'empêche pas l'autonomie.

La décennie précédente a été jalonnée de ces événements qui, par accumulation, ont jeté la lumière sur un impensé européen, recouvrant une dépendance généralisée non seulement aux géants du numérique, mais aussi au droit des puissances étrangères, fussent-elles alliées.

20 Définition tirée de l'encyclopédie libre Wikipedia

CLOUD

Le Cloud européen, une alliance de règles juridiques et techniques pour en garantir la souveraineté

La portée extraterritoriale d'une loi constitue par définition un risque majeur pour un Cloud souverain européen. Face à cette menace invisible, comment s'organiser ? Comment garantir un espace sécurisé aux entreprises utilisatrices du Cloud ? Au niveau juridique, comment mobiliser la norme, la loi et le contrat pour garantir la sécurité des pratiques au sein d'un Cloud de confiance ? D'une part, s'il convient avant tout d'éviter une inflation législative, la construction d'une nouvelle norme, autrement dit d'un nouveau droit de la donnée pourrait s'avérer une piste intéressante à condition de se structurer en veillant à ne pas faire de choix antinomiques. Des questions d'harmonisation se poseront alors pour éviter toute contradiction avec des textes existants ; les deux logiques européennes de libre circulation d'une part, et de protection d'autre part, devront notamment être prises en compte. Le contrat constitue, d'autre part, un second type d'instrument utile. Des clauses contractuelles spécifiques au contrat peuvent permettre de se prémunir de risques d'ingérence au niveau des données notamment. Néanmoins, les clauses d'un contrat n'engagent que les parties au contrat, signataires. D'une certaine manière, un contrat peut devenir stérile dès lors qu'un Etat souhaite appliquer ses lois ; seules, des clauses contractuelles ne permettent donc pas de se prémunir entièrement de l'extraterritorialité du droit.

La puissance normative de l'Europe – la loi – ou les clauses contractuelles – le contrat – sont-elles suffisantes pour appréhender tous les risques ? Suffiront-t-elles, aussi bien pensées soient-elles, à empêcher l'application de lois extraterritoriales ? Pour y parvenir, le droit doit s'organiser autour de standards techniques qui assurent le respect des lois et des contrats. C'est une alliance de dispositifs juridique et technique qui créera les conditions d'une protection efficace des services proposés au sein du Cloud de confiance.

Finalement, trois ensembles se mêlent et doivent poursuivre le même objectif : la loi, le contrat et les standards. L'alignement de ces trois sous-ensembles peut constituer un gage de souveraineté.

Un périmètre à clarifier : de quelles données parle-t-on ?

Historiquement, l'Europe et ses États membres se sont efforcés d'apporter un cadre réglementaire à la question des données personnelles. Par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[21], la France pose un premier cadre protecteur et crée la CNIL. En 1995, l'Europe adopte une directive sur la protection des données, la directive 95/46/CE[22]. En 2016, en remplacement de la directive de 1995, l'Union européenne adopte le RGPD pour renforcer notre droit à la protection des données. Au cœur de ces intentions législatives réside la protection des données ; elles ont d'ailleurs souvent été critiquées au motif qu'elles freinaient l'innovation. Pourtant, le RGPD comme le règlement européen relatif aux données non personnelles, adopté le 14 novembre 2018, visent d'une part à protéger les données et d'autre part à favoriser, via le libre flux des données, des innovations. Ainsi le règlement européen de 2018 supprime des règles nationales qui imposaient des exigences de localisation des données. En encourageant la mobilité des données, ce texte participe à la volonté de construire un espace européen commun de la donnée. Ce dernier s'inscrit naturellement dans l'esprit des libertés de circulation qui unifient économiquement l'Europe.

Les données d'entreprises sont souvent qualifiées de données dites sensibles, c'est-à-dire hautement confidentielles. Pourtant, le terme « sensible » correspond à une dénomination juridique utilisée dans le RGPD. La Commission nationale de l'informatique et des libertés le rappelle d'ailleurs :

« *Les données sensibles forment une catégorie particulière des données personnelles. Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* »[23].

Quelles conclusions en tirer s'agissant des données industrielles / privées ? Quelle qualification juridique et texte de référence pour ces données-là ? Le Data Governance Act peut-il répondre à ces interrogations ? « *Comment harmoniser les textes afin qu'il y ait, au moment de l'analyse des données et surtout lors de croisements de données personnelles et non personnelles, le moins de contradictions* » Adrien Basdevant - Basdevant Avocats, CNNum.

21 *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

22 *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AFR%3AHTML*

23 *https://www.cnil.fr/fr/definition/donnee-sensible*

Un Cloud souverain doit l'être sur toutes les couches

En cherchant des critères de souveraineté, l'Europe exprime sa volonté de lancer une politique industrielle numérique commune. Comme le rappelle un rapport sénatorial[24], « *la France comprend plusieurs champions sur les couches IaaS du Cloud (OVH, Atos, Orange Business Services ou encore Outscale), qui s'appuient sur un marché national en forte expansion pour attaquer le marché international* ». Toutefois, si la position française sur le marché du IaaS semble compétitive, le marché des services applicatifs (SaaS et PaaS (NLP, SpeechToText, API, OCR, ...)[25] reste largement dominé par les acteurs américains, avec en tête de file les fournisseurs Microsoft, Salesforce, Adobe, SAP ou encore Oracle. De manière globale, la domination américaine sur le marché mondial du Cloud est nette : Amazon Web Services reste leader avec une part de marché de 32% en 2020[26], devant Microsoft Azure (19%), Google Cloud Platform (7%) et Alibaba (6%). Gartner apporte un éclairage plus précis sur ce marché en différenciant les services d'infrastructure (IaaS, *Infrastructure as a Service*), les services de plateformes et de Serverless (PaaS, *Platform as a Service*), et les logiciels délivrés sous forme de services (SaaS, *Software as a Service*). En 2019, ils évaluaient le marché du IaaS à 44,5 milliards de dollars, soit une augmentation de 37,3% par rapport à 2018[27].

Face à ce constat, l'objectif de recherche de critères de souveraineté pour le Cloud européen est-il de soutenir un acteur capable de concevoir une solution européenne souveraine, ou à l'inverse, de proposer des solutions logicielles souveraines pour les entreprises utilisatrices ? Ou encore, de faire émerger un recueil d'exigences pour les opérateurs de données européennes, permettant la labellisation des solutions du marché pour un usage dans un contexte européen ? La volonté de créer un Cloud de confiance doit néanmoins être envisagée à l'aune des différentes couches d'un Cloud et du degré de risques de chacune de celles-ci. C'est le prisme par lequel nous abordons ce livre blanc en observant les acteurs, les réglementations et les solutions techniques sur chacune des couches.

24 *Le devoir de souveraineté numérique, rapport sénatorial de M. Gérard Longuet, octobre 2019*

25 *Software as a Service en anglais, logiciel en tant que service en français*

26 *AWS reste le maître du marché Cloud*

27 *Gartner évalue le marché mondial du IaaS à 44,5 milliards de dollars (itforbusiness.fr)*

Dans cet environnement, le Cloud souverain n'existe pas (encore)

L'Europe s'est historiquement organisée comme un espace de liberté de circulation : libre-circulation des biens, des personnes, des services et des capitaux. Appliquer ce principe structurant de la construction européenne en créant un espace européen de la donnée semble donc une évolution logique au regard de l'importance qu'occupent aujourd'hui les données. C'est le pas franchi par la Commission européenne le 14 novembre 2018 qui donne naissance à cette cinquième liberté[28]. Assurément, dans sa stratégie en matière de données dévoilée au début de l'année 2020, la Commission européenne précise d'ailleurs que « *le volume croissant de données des secteurs privé et public à caractère non personnel en Europe, combiné à l'évolution technologique pour le stockage et le traitement des données, constituera une source potentielle de croissance et d'innovation dont il convient de tirer parti* » : c'est notamment dans ce contexte que s'inscrit le projet de Cloud de confiance.

Reprendre le contrôle de notre souveraineté numérique, aux niveaux français et européen, suppose d'avoir le choix entre différentes solutions technologiques. Le projet GAIA-X, dont l'objectif principal est d'offrir une alternative aux solutions proposées par les géants américains de l'hébergement de données, communément appelés hyperscalers, répond en ce sens à une volonté européenne partagée de reconquête numérique. Pourtant, force est de constater qu'en matière d'offres Cloud, les grands acteurs du numérique américains et chinois, avec en tête de file *Amazon Web Services, Microsoft Azure, Alibaba Cloud, Google Cloud et Tencent Cloud,* dominent nettement le marché. A titre d'exemple, ces cinq acteurs représentaient 80% du marché du IaaS[29] en 2019[30].

S'il est légitimement perçu comme une opportunité économique par les parties-prenantes impliquées, l'objectif d'un Cloud de confiance à l'échelle européenne semble résolument stratégique. La volonté européenne de développer des capacités Cloud s'inscrit ainsi dans une démarche géopolitique visant à limiter la dépendance européenne aux acteurs américains et chinois. Néanmoins, la pluralité des définitions du terme souveraineté numérique décrit précédemment complique la définition d'un Cloud souverain. Comment le Cloud européen, incarné aujourd'hui par GAIA-X, peut-il être considéré comme souverain sans une définition juridique européenne de la souveraineté numérique ?

Doit-il l'être ? Comment peut-il y parvenir ? A cette question, Olivier Senot, Directeur de l'innovation, Docaposte ; répond sans ambiguïté :

« *Est-ce que GAIA X est un cloud souverain ? Bien malin qui peut donner une réponse juridique claire. Je pense qu'elle n'existe pas. En revanche il a été établi un certain nombre de règles avec un focus clair : garantir aux entreprises qu'elles garderont la maîtrise des données exploitées ou utilisées par les tiers* »

Faut-il parler de Cloud souverain versus de Cloud de confiance ?

SOUVERAINETÉ DU CLOUD

Servane Augier (VP Développement et Affaires Publiques 3DS OUTSCALE, membre du board de GAIA-X et membre du bureau d'Hexatrust), en février dernier, devant la Mission d'information de la Conférence des Présidents, sous la direction de Philippe Latombe, a donné sa définition de la souveraineté du Cloud.

Dans ses propositions, elle insiste particulièrement sur les points suivants :

- la «territorialisation» du stockage et de l'opération des données de leurs clients (en France et plus largement en Europe)
- la signature du contrat avec les clients en droit français. Servane Augier a commenté ultérieurement ce point en insistant sur l'intérêt d'indiquer de façon explicite dans les Conditions Générales de Vente, le cadre réglementaire auquel est soumis le fournisseur. Cette idée avait déjà été soulevée auprès du comité stratégique de filière de la DGE.
- l'utilisation d'un Cloud de confiance pour l'hébergement des données sensibles pour les administrations et les OIV
- Plus largement, la mise en place d'un label « Cloud de confiance », à la manière des référentiels techniques.

A ce sujet, Servane Augier précise que le 29 mars dernier, l'Association GAIA-X a annoncé la création d'un prochain label attribué aux services ou produits qui sont conformes aux principes et spécifications de GAIA-X notamment en matière de conformité au droit européen, portabilité, sécurité, réversibilité et transparence en matière d'utilisation des données. Ce label pourra être décerné aussi bien aux membres qu'aux non-membres de l'Association.

Sur le Cloud Act, elle souligne la nécessité de sortir de l'emprise actuelle, sur nos données, des réglementations extra-européennes. Elle ajoute «Dans le contexte réglementaire actuel, la souveraineté s'entend comme n'étant pas soumise à des réglementations extra-européennes. On ne peut pas prétendre être souverain quand on est soumis au Cloud Act » En ce sens, la souveraineté numérique repose sur une souveraineté juridique.

28 La libre circulation des données est devenue la cinquième liberté consacrée dans le droit de l'Union européenne

29 Infrastructure as a Service en anglais, Infrastructure en tant que Service en français

30 Gartner évalue le marché mondial du IaaS à 44,5 milliards de dollars

> “ Le Cloud est la technologie qui commande toutes les autres : Edge Computing, IA, 5G,... toutes se développent sur le Cloud ”
>
> Henri d’Agrain – Cigref.

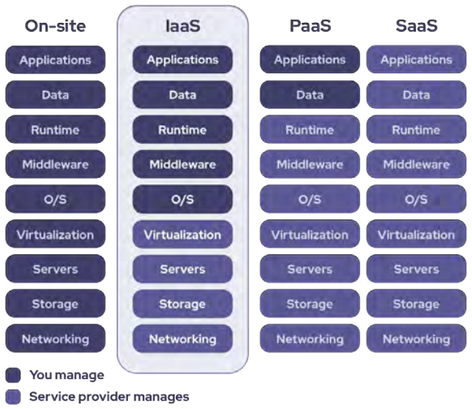
Définir le Cloud souverain c’est donc définir le fondement de la souveraineté numérique, et comme souvent, deux approches complémentaires se répondent et parfois s’éclipsent. Cela étant, fixer la notion de Cloud souverain est problématique, non seulement du fait de l’absence de sa définition juridique, mais aussi du fait de l’impossibilité, en l’état actuel, de maîtriser tous les acteurs et composants de la chaîne de valeur d’un service Cloud. En ce sens, et en accord avec les participants, il est sans doute préférable de parler d’un Cloud caractérisé par la confiance qu’il suscite grâce à un certain nombre d’exigences qui, mises bout à bout, construisent le chemin vers la souveraineté numérique.

La souveraineté numérique, c’est notre capacité à maîtriser nos dépendances aux solutions technologiques extra-européennes, à garantir l’autonomie stratégique des États et de leurs entreprises. Mais c’est aussi la capacité à ne pas se laisser imposer une certaine vision du numérique, et à garder notre propre pouvoir d’influence politique dans le monde qui se dessine sous nos yeux.

À l’instar du RGPD qui défend les droits des personnes et sécurise leur bien le plus précieux sur internet, à savoir leurs données, le règlement européen promeut également les valeurs humanistes de l’Union européenne. Ainsi en s’imposant comme cadre référent au niveau mondial, le RGPD sécurise notre propre marché, et impose nos standards aux grands ensembles géopolitiques, qu’ils soient publics ou privés.

La définition du Cloud européen porte en elle cette dichotomie, avec d’un côté ceux qui préfèreront entendre la défense d’un nouveau standard numérique mondial protecteur de nos valeurs, et ceux qui y verront un cadre technologique d’une cyber défense commune européenne. Dans les deux cas, il s’agit bien d’un Cloud de confiance qui garantit notre sécurité technologique et juridique, et protège nos principes humanistes. Et ce faisant consolide une offre européenne alternative aux hyperscalers, et bâtit les fondements d’un marché unique de la donnée.

Cloud de confiance



Source : L’infrastructure en tant que service (IaaS), qu’est-ce que c’est ?

PROPOSITIONS DE SOLUTIONS

Afin d'éviter le piège décrit en introduction du mot « souverain », nous avons décidé d'articuler nos propositions autour de la notion d'« autonomie stratégique », permettant ainsi une approche plus constructive des enjeux.

Au gré de nos auditions, nous avons collectivement constaté qu'il ne pouvait y avoir d'autonomie stratégique sans : autonomie technologique, autonomie décisionnelle, et avant tout, sans autonomie éducative. Des propositions seront faites pour soutenir chaque forme d'autonomie.

En participant à ce livre blanc, nous nous sommes impliqués pour nos entreprises au nom de nos intérêts communs, mais aussi au nom de l'intérêt général pour une question qui dépasse les simples enjeux économiques.

A travers le Cloud se dessine une certaine vision du numérique, une problématique hautement stratégique qui détermine nos choix et nos possibles.

De nos discussions sont nées des convictions, parfois des solutions, des pistes que nous pensons devoir emprunter.

En les partageant nous les offrons au débat mais surtout nous les exposons à l'action.

Nous y prendrons toute notre part en restant acteurs, parfois moteurs, de cet engagement que nous continuerons d'alimenter en les faisant vivre au sein de nos entreprises, filières et écosystèmes.

Voici ces propositions.

Autonomie technologique

- Comprendre et contrôler l'intégralité de la chaîne du Cloud ;
- Favoriser l'essor et le soutien sur le long terme de l'open source ;
- Renforcer les travaux de recherche sur le Edge en vue de leur transfert vers des acteurs européens clés ou vers l'association GAIA-X ;
- Coordonner les dimensions transverses (sécurité par exemple) et promouvoir un encadrement européen qui intègre l'ANSSI et l'ENISA ;
- Intégrer les labels de « transparence » dans les AO ;
- Faire évoluer les référentiels actuels afin d'inclure la prestation Cloud dans les OIV - OSE ;
- Renforcer la position des tiers de confiance.

Autonomie décisionnelle

- « Tiers d'arbitrage » pour chaque espace de données sectoriel du Cloud souverain ;
- Identifier les actions de concurrence déloyale et notamment les « ventes liées » ;
- Renforcer les critères environnementaux dans les appels d'offre ;
- Conforter notre autonomie stratégique par un lobbying approprié.

Autonomie pédagogique

- Création d'un dispositif d'accompagnement spécifique pour les décideurs : décoder, décider ?
- TOIEC du Cloud.

AUTONOMIE TECHNOLOGIQUE

En introduction de ce chapitre consacré à l'autonomie technologique, les contributeurs ont insisté sur trois éléments de contexte que nous détaillerons tout à tour et qui permettent d'éclairer les propositions faites dans ce document.

L'observation des investissements actuels mondiaux en matière de modernisation du numérique

Pour faire face aux cybermenaces, le gouvernement français a mobilisé 1 milliard d'euros. Cette somme est à mettre en regard des investissements réalisés aux États-Unis et notamment le plan de 10,2 milliards de dollars voté par l'administration Biden, qui a pour objectif de moderniser le socle numérique fédéral en s'attaquant à plusieurs chantiers : la sécurité des identités, les accès et les architectures IT. « *Après l'attaque SolarWinds (qui a touchée de nombreuses entreprises privée et publiques dans le monde en s'infiltrant via l'éditeur de logiciel américain SolarWinds), l'« American RescueAct » doit permettre au gouvernement américain de reprendre le contrôle de toutes ses infrastructures informatiques, avec en particulier le contrôle du mot de passe « root » et la sécurité des couches applicatives où seront déployées les futures applications fédérales américaines* » souligne Jean-Noël de Galzain[31].

Les propositions actuelles d'encadrement des GAFAM

La définition actuelle des gatekeepers proposée par les règlements DMA rend possible l'identification des acteurs concernés. Ce nouveau cadre de responsabilité doit permettre à l'Europe de : « *promouvoir son propre modèle, fidèle à ses valeurs, qui se distingue des modèles existants de « laisser-faire » d'une part, ou de contrôle et de surveillance. Elle doit construire un modèle de régulation ambitieux, durable, où la concurrence est préservée, et qui fasse référence dans le monde* »[32].

« *Ainsi, l'enjeu historique est bien de reprendre le contrôle des infrastructures et des architectures IT, dans le monde entier, tout en renforçant la sécurité by design. C'est l'une des clés de ce que l'on appelle la souveraineté numérique* » Jean-Noël de Galzain – Hexatrust

31 Global_Security_Mag_20210314110000 (kmni.eu)

32 Grandes plateformes du numérique : vers le Digital Services Act et Digital Markets Act | economie.gouv.fr

“Les projets européens DSA-DMA doivent poser le cadre de régulation pour les vingt prochaines années. Il importe que des acteurs devenus structurants endossent des responsabilités correspondant à leur pouvoir de marché effectif. Ils ne sauraient se retrancher plus longtemps derrière des statuts artificiellement protecteurs, sans rapport avec leur puissance économique réelle”

15 décembre 2020 – Cédric O – secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques.[1]

1 Download (augure.com)

Le développement du Edge Computing et ses opportunités

A l'ambition première du Cloud de confiance, celle de réunir au sein d'un écosystème numérique ouvert des données pouvant être partagées, s'ajoute une seconde ambition, celle d'intégrer toutes les révolutions liées au Cloud, notamment l'internet des objets et le *Edge Computing*.

Comme le précise un rapport de la Commission européenne datant de février 2020, « *80 % des opérations de traitement et d'analyse des données se déroulent dans des centres de données et des installations informatiques centralisées, et 20 % dans des objets connectés tels que des voitures, des appareils ménagers ou des robots de l'industrie manufacturière, ainsi que des installations informatiques proches de l'utilisateur. D'ici à 2025, ces proportions vont probablement s'inverser* ».

L'intégration des acteurs de l'informatique en périphérie de réseau constitue un facteur clé de succès pour un Cloud de confiance. Ce faisant, l'Europe pourrait favoriser la création d'un écosystème européen puissant sur les technologies de Edge Computing.

Au regard de ces différents constats, l'autonomie technologique repose sur un certain nombre de leviers sur lesquels nous pouvons nous appuyer. Observons ici les principaux.

Une infrastructure capable de supporter des outils souverains

Le Cloud est-il plus grand que la somme de ses parties ?

Le Cloud est souvent abordé dans sa globalité. Cette approche est une force car elle permet de traiter le Cloud comme une chaîne de valeur complète et contribue à n'abandonner aucune de ses parties et particulièrement le marché du SaaS qui peine à trouver sa taille critique en Europe.
Le modèle SaaS s'avère être un pari économiquement gagnant. Il assure aux entreprises un chiffre d'affaires plus stable et récurrent. « Selon les données récoltées récemment par Gartner, près de 70% des organisations utilisant des services Cloud prévoient aujourd'hui d'augmenter leurs dépenses consacrées dans ce domaine en raison des perturbations provoquées par le Covid-19. Le logiciel en tant que service (SaaS) restera le plus grand segment de marché pour atteindre 117,7 milliards de dollars en 2021[33] »

33 Le marché des services de Cloud public devrait progresser de près de 20% en 2021 selon Gartner

> **D'ici 2023, plus de 500 millions d'applications et de services numériques seront développés et déployés à l'aide d'approches Cloud natives".**
>
> IDC FutureScape: Worldwide IT Industry 2020 Predictions, Oct 2019

Les challenges sont donc multiples et concernent des publics différents. Ainsi le développeur se concentre sur le code logiciel de l'application sans se préoccuper de l'infrastructure, l'utilisateur devOps automatise les ressources d'infrastructure et veille à offrir un bon niveau de service aux applications tandis que l'utilisateur final a besoin d'une application métier qui fonctionne au meilleur prix et dans le respect de la sécurité des données.

C'est pour répondre à ces différents besoins qu'OVHCloud et Google Cloud ont annoncé un partenariat stratégique pour co-construire une solution de Cloud de confiance en Europe. Il s'agira d'offrir une infrastructure OVHCloud où les applications des clients s'exécuteront et où les données seront stockées. Ainsi la suite logicielle d'Anthos basée sur de l'Open-source et qui comprend : *Anthos Cloud run* (container-as-a-service «Serverless», simplifie l'expérience du développeur, déclencheurs d'évènements), *Anthos Service Mesh* (facilite l'architecture orientée services / microservices (observabilité, sécurité / tests ...) et *Anthos Kubernetes Engine* (distribue, garantit la haute disponibilité et fait évoluer les logiciels conteneurisés de manière intelligente sur l'infrastructure), sera disponible de façon sécurisée.

Pourtant dissocier la couche infra des autres couches apparaît vite comme la solution. « *Il faut chercher dans cette direction et découpler la partie infrastructure, stockage de données et capacité de calcul de tous les services que les clients adoptent rapidement dans les offres Cloud actuelles* » Jérôme Martin – BearingPoint.

Olivier Senot - Docaposte – ajoute « *La communauté internationale est très active sur la recherche des failles, et notamment sur le fait qu'un environnement technologique (stack) soit ou ne soit pas souveraine quand elle est installée sur un IaaS. La séparation de cette pile de l'ensemble IaaS est une solution* ».

Au-delà de l'infrastructure, c'est bien la donnée qu'il faut prendre en compte dans toutes ses acceptions. Nous pouvons l'aborder de plusieurs façons : « *Elle peut être stockée, dans son état le plus simple ou faire l'objet de traitement par des logiciels et matériels tiers. Elle passe alors dans un état qui peut être beaucoup plus complexe. Cette donnée a aussi un poids important dans l'équation car elle est posée sur des composants logiciels, et ces composants sont posés sur un socle IaaS dont il faut garantir la souveraineté. Je pense que le point focal est la donnée et répondre à la question : Comment s'assurer qu'une donnée dans tous ses états puisse rester dans un environnement de confiance ?* » Olivier Senot Directeur de l'innovation, Docaposte.

LA RÉPONSE D'OVHCLOUD ET DE GOOGLE CLOUD 10 NOVEMBRE 2020

OVHCloud hébergera et traitera la technologie logicielle Anthos de Google, entièrement intégrée à l'infrastructure d'OVHCloud. Cela a pour objectif d'aider les organisations européennes à accélérer leur transformation commerciale dans le Cloud et à répondre à leurs exigences strictes en matière de sécurité des données et de confidentialité.

L'Open source une réponse qui ne peut s'affranchir de considérations géopolitiques

Dans les nombreux paradoxes du Cloud, celui du développement logiciel par des communautés open source[34] en est un. Seules ces communautés sont aujourd'hui suffisamment compétitives et offrent la vélocité nécessaire pour s'adapter aux attentes des clients, face à des géants comme les hyperscalers. « *Il faut arriver à construire avec l'existant et l'existant, ce sont des communautés internationales open source. Cela peut sembler contradictoire avec la notion de souveraineté* » Frédéric Desprez – INRIA

L'intérêt de l'open source est, via la disponibilité du code source, son auditabilité. La disponibilité de ce code source est ou pourrait être plus régulièrement exigée dans les contrats. Elle serait une garantie de qualité sur la partie logicielle. Cela peut sembler plus compliqué sur la partie matérielle.

D'autres avantages sont ici rappelés par les personnes interrogées : la baisse significative des coûts, la moindre dépendance à un fournisseur unique et une qualité globale souvent supérieure du fait de corrections plus rapides.

Le développement d'un standard à partir de solutions open source apparaît comme une première réponse à la nécessité de disposer de piles logicielles identiques sur les couches basses. Il sera plus facile ensuite de déployer, au-dessus, un ensemble de services :

« *Des réflexions sur des use cases Edge sont en cours et rassemblent depuis plus de cinq ans une multitude d'acteurs... en termes d'infrastructure de calcul et de stockage, ce que nous désignons comme la partie du Cloud la plus proche des usagers, nous avons encore une carte à jouer* » Adrien Lèbre Professeur – IMT Atlantique.

La question du financement des développements logiciels est posée et nécessite un investissement fort des sociétés européennes lors des levées de fonds « *Les salariés ne disposent pas de temps pour participer à des développements open source. Ils consomment beaucoup de Kubernetes mais cela s'arrête là* » Raphaël de Cormis – Thalès.

Les raisons sont-elles aussi juridiques ? « *Les licences libres présentant un copyleft fort s'imposent à l'ensemble du logiciel. Elles obligent toute personne qui travaille sur la diffusion d'un logiciel dérivé d'une brique logicielle placée sous cette licence (dite contaminante), à la respecter* ». Raphaël de Cormis – Thalès.

Dans les autres raisons évoquées, est souvent citée l'initiative européenne OpenNebula. Ce système a perdu la bataille du IaaS Open Source qui est aujourd'hui largement piloté par la pile OpenStack, pile logicielle Open Source notamment utilisée pour opérer l'ensemble des centres de données d'OVHCloud.

« *OpenNebula et les autres solutions sont en perte de vitesse parce que le débat s'est déplacé. Il n'est plus au niveau de l'infrastructure mais au niveau de la gestion du cycle de vie des applications qui sont sur des infrastructures Cloud, que ce soit du Cloud centralisé ou du Cloud Edge* » Frédéric Desprez – INRIA.

Enfin et surtout L'open source pose la question des pays contributeurs car, comme le rappelle Servane Augier – Outscale « *L'open source ne peut s'affranchir de réalités géopolitiques* ». La localisation du développeur n'est pas anodine comme le rappelle l'exemple de RISC V. Leur fondation s'est implantée en Suisse en 2019 suite aux pressions américaines qui souhaitaient leur interdire de travailler avec des entreprises chinoises. La même année,

34 Introduction The Open Source Model Europe's Largest Open Source Organization

« *Sur GAIA X, des composants open source sont créés et leur maintien est sous la responsabilité du CTO. C'est la fondation ECLIPSE*[1] *qui va gérer la question de l'API. De la même façon, les data spaces vont développer des composants en open source. Ce sont les consortiums de users qui vont porter les développements en lien avec l'association GAIA X* ». Olivier Senot – Docaposte.

1 https://www.eclipse.org/europe/eclipse-fact-sheet.pdf

le géant du commerce en ligne Alibaba a lancé son propre processeur Xuantie 910 basé sur l'architecture open source RISC V, afin de contourner les tentatives de l'administration Trump de limiter les fournitures de puces.

La prise en compte de l'avènement du Edge Computing

Les entreprises françaises ont très tôt fait le pari du Edge parfois également appelé Fog Computing. « *Les deux formulations évoquent le déplacement du Cloud centralisé dans des méga centres de données vers une infrastructure plus géo-distribuée ayant vocation à rapprocher le traitement et le stockage au plus près des usagers* ». Adrien Lèbre – Professeur IMT Atlantique

Nous rappelions plus tôt dans cette partie du livre blanc que la puissance d'innovation se partage entre les grands groupes et les startups. Le développement du Edge Computing va logiquement voir le nombre de fournisseurs de capteurs augmenter ; si ceux-là se structurent avec des pratiques et des standards distincts de ceux choisis par le Cloud de confiance, des problématiques de partage de valeur et de sécurité émergeront.

Adrien Lèbre – Professeur IMT Atlantique – souligne « *Il n'y a pas aujourd'hui de solution qui permette à un nouvel acteur, type opérateur télécommunication, de se positionner comme un nouveau fournisseur d'infrastructure Edge. Plusieurs groupes de travail existent et avancent vers un tel objectif (Edge Computing de l'Openstack Foundation, ETSI MEC, Edge Working group dans l'écosystème Kubernetes etc…). Toutefois, les propositions sont encore loin d'offrir les fonctionnalités qui ont fait le succès du Cloud (c'est-à-dire cette capacité à déployer à la demande et n'importe où sur le continuum Cloud/IoT des ressources de calculs/stockages etc.) Enfin, je ne pense pas qu'il faille opposer le Cloud au Edge. Le Edge expose les infrastructures de prochaines générations comme un continuum entre le Cloud et l'IoT. Il y aura donc encore des traitements qui se feront dans le Cloud (i.e. de très gros datacenters), le Edge étant là pour limiter la remontée des informations vers ces gros mastodontes* »

Rappelons ici que les règles et les standards notamment en matière d'infrastructure, proposés dans le cadre de GAIA-X comportent un chapitre dédié à la portabilité et à l'interopérabilité dans lequel se trouve la mention du Edge Computing, en ces termes « *As a possible processing paradigm to create possibilities for real-time processing and distributed algorithms, Cloud native apps vs. Edge apps* ».

> "Au sein de GAIA-X, L'IoT industrielle va se déployer en même temps que la 5G industrielle et la question du Edge Computing va être au cœur des préoccupations"
>
> Olivier Senot – Docaposte

Une des propositions évoquées serait de réfléchir à la mise en place, au sein de GAIA-X d'un groupe de travail dédié uniquement à la question du Edge Computing, en intégrant à la réflexion des fournisseurs de Cloud – ils vont être impactés par le développement du Edge – des acteurs de l'industrie 4.0 – ils vont avoir recours aux IoT et au Edge à tous les niveaux – et des entreprises du secteur télécom.

Vers une co-création de standards européens dans le Cloud

CHIFFRES CLÉS TOUR D'HORIZON DU MARCHÉ DU EDGE COMPUTING

43,4 milliards de dollars

La taille du marché mondial de l'Edge Computing explosera à ce niveau d'ici 2027 – soit un taux de croissance annuel composé de 37,4 % - Grand View Research

29 milliards de dollars

C'est le nombre prévu d'appareils connectés qui se disputeront l'attention du réseau mondial d'ici 2022, selon la Telecommunications Industry Association. Plus de la moitié d'entre eux (18 milliards) seront des appareils IoT.

30% en moyenne

Les données d'enquête suggèrent que les entreprises consacreront en moyenne 30 % de leur budget informatique au Cloud Computing au cours des trois prochaines années, selon « Strategies for Success at the Edge, 2019 », rapport d'Analyse Mason.

57% des décideurs

en matière de mobilité déclarent avoir l'Edge Computing sur leur feuille de route au cours de l'année prochaine, en réponse à l'enquête 2019 Forrester Analytics Global Business Technographics Mobility Survey

Gartner prévoit que d'ici 2025, les **trois quarts des données générées par les entreprises** seront créées et traitées dans l'Edge – en dehors d'un centre de données centralisé traditionnel ou du Cloud. Ce chiffre est en hausse par rapport à seulement 10 % en 2018.

Dans le prolongement de l'Open Source, la première étape serait l'adoption de réglementations et de principes de mutualisation. C'est le choix de GAIA-X, comme le souligne Olivier Senot – Docaposte « *Mutualiser les sociétés permet de mobiliser suffisamment de ressources pour développer une solution dans un temps court. C'est l'orientation et la philosophie prises au sein de GAIA-X. L'objectif poursuivi par les appels à projets nationaux et européens est que des consortiums de sociétés se forment pour répondre, dans une période de temps donnée, à une problématique précise. De ces collaborations naîtront, des solutions pertinentes et up-to-date par rapport à la concurrence. C'est dans cet état d'esprit que GAIA-X ; avec le besoin des utilisateurs comme guide ; progresse dans la démarche de mise à disposition d'un Cloud de confiance transparent sur les acteur technologiques traitant la donnée* ».

Dans les solutions avancées, la régulation occupe une place importante notamment en matière d'infrastructures autour du Edge Computing. Ces dernières seraient pilotées par des acteurs européens. Les hyperscalers pourraient proposer à la vente ou à la licence leurs logiciels sans opérer la partie infrastructure.

Le Edge Computing va s'imposer car « *techniquement, aujourd'hui, nous ne pouvons pas analyser le flux de 10 000 caméras en 4 K. Les volumétries sont trop importantes. De plus avec la réalité augmentée ou le véhicule autonome connecté, les exigences en matière de réactivité et donc de diminution des temps de latence, sont critiques. Nous devons donc être en mesure de piloter et d'exposer des ressources de type Edge pour l'IoT* » Adrien Lèbre – Professeur IMT Atlantique.

Le roaming, peut-être aussi une source d'inspiration pour le computing. Cette analogie permettrait, par la voie réglementaire, d'obliger les acteurs à travailler ensemble plutôt que de les mettre en compétition.

Le roaming ou itinérance est défini par l'ARCEP (Autorité de Régulation des Communications Électroniques et des Postes) dans l'exemple suivant :

« *Un client d'un opérateur mobile français qui utilise son téléphone mobile lors d'un déplacement à l'étranger se retrouve en situation « d'itinérance » ou de « roaming » sur le réseau d'un opérateur mobile étranger. Chaque minute de voix, SMS ou Mo consommé utilise ainsi les ressources du réseau de cet opérateur étranger, qui facture des frais d'utilisation de son réseau à l'opérateur français d'origine du client*[35] ».

35 L'itinérance internationale («roaming»)

De la même façon, il s'agirait d'assurer d'une part une bonne interopérabilité entre les solutions logicielles. Elle pourrait s'accompagner d'une volonté claire de séparer la partie « calcul » de la partie « hertzienne » afin de garder une souveraineté sur l'infrastructure de communication « *qui demain sera le socle de toute activité car le réseau est déjà la racine de toute activité* » Olivier Senot – Docaposte.

Ces réflexions pourraient aboutir à d'autres propositions comme la création d'une agence européenne liée au déploiement du calcul sur la 5G. Cette agence travaillerait à formaliser un certain nombre d'exigences, à rationaliser le déploiement du hardware comme le font les réseaux NREN* et à réguler le marché.

***L'EXEMPLE DU RÉSEAU NATIONAL DE TÉLÉCOMMUNICATIONS POUR LA TECHNOLOGIE, L'ENSEIGNEMENT ET LA RECHERCHE (RENATER)**

Il fédère les infrastructures réseau pour la recherche et l'éducation. Ce réseau sécurisé à très haut débit pouvant dépasser 100 Gbps sur certains axes, fournit une connectivité nationale et internationale dédiée à plus de 2 millions d'utilisateurs et à travers 1400 sites d'enseignement et de recherche. Ses missions sont :

- de fournir aux acteurs de la communauté recherche et éducation les moyens de communication numérique haut débit et de gestion des données liées en France (métropolitaine, dans les ROM et dans les COM) sur la base de réseaux, d'infrastructures et de services ;
- d'assurer que l'ensemble de ces moyens sont sécurisés ;
- d'assurer l'interconnexion aux réseaux de recherche et éducation mondiaux ;
- d'assurer les travaux des équipes en réseau et de répondre aux besoins avancés et innovants de la communauté recherche et éducation ;
- d'assurer une mission de conseil, d'expertise, de fournir des moyens ou des services de communication dans ses domaines de compétence auprès de l'État et d'autres entités publiques français ou étrangers, dans la mesure où cela n'impose pas au Groupement des obligations incompatibles avec sa mission de fourniture de services à la communauté recherche et éducation[1].

Au niveau européen, le réseau GEANT2 regroupe 30 millions d'utilisateurs issus de 34 pays européens. Le projet est mené par un consortium constitué de 32 NREN (National Research and Education Network, réseaux nationaux pour l'enseignement et la recherche) et de l'association TERENA (Trans-European Research and Education Networking Association), la coordination du projet étant assurée par DANTE (Delivery of Advanced Network Technology to Europe) : Organisation qui vise à la mise en place de réseaux de recherche partout dans le monde. Le projet GÉANT2 (nom de code : GN2) est cofinancé par la Commission européenne.

1 https://www.enseignementsup-recherche.gouv.fr/cid99660/www.enseignementsup-recherche.gouv.fr/cid99660/reseau-national-de-telecommunications-pour-la-technologie-l-enseignement-et-la-recherche-renater.html

La traçabilité mise en œuvre dans le transport aérien : une analogie à creuser en matière d'auditabilité et de transparence

François Desnoyer – Safran Landing Systems, propose ici de considérer l'internet comme « *une infrastructure mondialisée permettant les échanges d'informations, la réalisation de transactions, ainsi que le déplacement virtuel des personnes à une échelle globale, et d'en faire la comparaison avec une autre grande infrastructure ayant supporté de manière comparable la mondialisation : le transport aérien* ».

C'est également un secteur fréquemment cité en exemple pour sa contribution à la souveraineté européenne et au développement de l'industrie. L'Europe possède ainsi des grands acteurs mondiaux, en capacité de concevoir et de produire sur son sol, ainsi qu'une capacité propre de production de matériel militaire et d'avions de combat, comme en témoigne le projet SCAF de futur avion de combat européen[36].

Les raisons pour lesquelles la plupart d'entre nous empruntent sans appréhension des aéronefs, ou les regardent passer sans crainte au-dessus de leur maison ne trouvent pourtant pas leur origine dans cette position de force géopolitique et ce succès économique. Elles sont plutôt le fruit de normes et standards de fonctionnement construits au fil des années, et appliqués à tous les acteurs de la chaîne de valeur de la filière aéronautique.

Des agences fédérales, comme la FAA (*Federal Aviation Administration*) ou l'EASA (*European Aviation Safety Agency*) ou des organisations internationales comme l'ICAO (*International Civil Aviation Organization*) ont parmi leurs missions de définir et de faire appliquer des normes sur tous les produits et process utilisés : matériels volants, logiciels, procédures de maintenance, d'opération, de pilotage… tout est normé, contrôlé, certifié, et auditable, avant et après la mise en service, pour un usage toujours plus sûr des infrastructures et matériels permettant le transport aérien.

Les principes de transparence, de traçabilité, et de déterminisme (il faut pouvoir produire la démonstration du comportement d'un système complexe avant sa mise en service) sont donc au cœur des activités de la filière, qui ne peut s'autoriser l'improvisation et l'approximation, au risque de conséquences possiblement catastrophiques. Lorsque des accidents surviennent, ils sont analysés et utilisés pour l'amélioration continue des pratiques aussi bien que pour la recherche de déviations éventuelles aux protocoles.

Il est intéressant de remarquer que ces principes n'entravent pas la libre circulation des personnes et des biens. Les faciliter est d'ailleurs l'une des missions constitutives de l'EASA. La concurrence reste quant à elle très forte entre les acteurs américains et européens : le duopole Airbus/Boeing et leurs supply-chain respectives sera bientôt rejoint au premier plan des

36 https://www.capital.fr/entreprises-marches/defense-lavion-de-combat-europeen-du-futur-scaf-embourbe-dans-les-rivalites-entre-industriels-et-grandes-puissances-1397590

acteurs de l'aéronautique chinoise. Quant au développement de produits militaires, s'il fait l'objet de contrôles très stricts de ses exportations, et de stratégies diverses selon les États. C'est donc un modèle qui semble intéressant pour illustrer les différences entre confiance, souveraineté économique, souveraineté militaire, indépendance stratégique, et pour montrer leur compatibilité dans une mise en œuvre politique.

Bien que limité tant les technologies et les usages sont différents, un parallèle peut donc être tenté entre les manières d'encadrer la contribution au développement de l'activité humaine de ces deux inventions majeures. Les principes d'auditabilité et de transparence semblent par exemple nécessaires pour contrôler le fonctionnement des logiciels et des matériels utilisés par les grands acteurs du numérique. Nous pourrions imaginer une mise en œuvre systématique à partir d'un nombre d'utilisateurs ou d'une quantité de données. Des agréments pourraient alors être délivrés par une agence de sûreté du web, chargée de prévenir les accidents de Cloud, dotée d'un pouvoir coercitif, et d'une capacité de former, labelliser, ou fédérer des acteurs de confiance. Ces pistes de solutions restent complètement à développer en intégrant notamment les nombreux organismes œuvrant déjà au bon fonctionnement du web (ICAN, …) ou au développement de la cyber sécurité (ANSSI…), ainsi que les initiatives open source ».

L'adoption de critères répondant à des enjeux de souveraineté

Identité et mécanismes de confiance

L'enjeu de confiance est une problématique centrale citée à tous les niveaux du Cloud et en premier lieu au sein de la « Stratégie Cloud » qui fait partie des marchés prioritaires du quatrième programme des investissements d'avenir. La première des priorités est de « *Renforcer notre souveraineté numérique en soutenant la création et l'usage de solutions de confiance, c'est-à-dire, de solutions qui protègent les données des citoyens, des entreprises et des administrations françaises, conformément aux valeurs européennes* »[37]. Cette notion de confiance est, elle aussi, au cœur des définitions de la cybersécurité : « *La cybersécurité est la capacité à protéger les données et les services proposés dans l'espace numérique contre des attaques susceptibles d'en compromettre la disponibilité, l'intégrité ou la confidentialité. Elle comprend : Un enjeu de confiance : les utilisateurs doivent pouvoir bénéficier des possibilités offertes par le numérique sans craindre pour la sécurité de leurs données, pour la disponibilité des services dont ils dépendent ou encore pour leur intégrité physique* »[38]. Quelles sont les réponses abordées par les contributeurs à ce livre blanc ?

Le contrôle continu via un tiers de confiance (organismes de certification, acteurs industriels ou cabinets de conseil) atteste de la chaîne de trust. C'est, d'une certaine manière, ce que propose le visa de sécurité délivré par l'ANSSI, SecNumCloud, qui permet d'évaluer selon des critères stricts la sécurité mise en place chez certains acteurs du marché. C'est aussi ce que propose AWS avec ses cinq rapports *AWS System Organization Control* (SOC). Ce sont des comptes rendus rédigés suite à un audit indépendant réalisé par un tiers et indiquant comment AWS parvient à mettre en œuvre ses principaux contrôles et objectifs en termes de conformité. Nous pourrions aller au-delà du rapport et élargir l'auditabilité en permettant au tiers de confiance de réaliser des tests impromptus.

La fédération des tiers de confiance du numérique « *Élabore des référentiels techniques, forme, participe à la mise en place d'une digitalisation sécurisée et fiable* »[39]. Créée en 2001, elle opère avec pertinence la fusion de la technologie avec le droit et le « chiffre ». Elle apporte au marché du Numérique un inestimable gisement de compétences dans les domaines historiques de la digitalisation : signature électronique, archivage électronique, identité numérique, facture électronique, vote électroniques, e-finance, e-santé, … mais également dans ses domaines montants : Blockchain, KYC, Cachet électronique visible (CEV). Elle est un exemple, notamment en matière de labels qui concernent à terme « *l'ensemble des services de confiance. Le premier à voir le jour a été, en 2004, le label FNTC-TA dédié aux services de tiers archivage* »[40].

Hubert Tardieu, président du Conseil d'Administration de GAIA-X, rappelle la définition de services tel que « *Identity & Trust* ». Il fournit un mécanisme pour identifier les entreprises et les fournisseurs de données ainsi que les mécanismes de confiance associés. C'est, souligne-t-il, un peu ce qu'Amazon/Google/Microsoft ont permis avec leurs authentificateurs[41].

Les enjeux d'un label « Cloud de confiance »

L'exemple des récentes annonces faites, dans le cadre de GAIA-X, est une bonne illustration des enjeux d'un label de confiance qui à terme pourrait être dupliqué dans d'autres organismes. Ainsi, « *GAIA-X sera capable de proposer en décembre 2021 les première solutions labellisées GAIA-X qui rendront plus facile la collaboration industrielle* » autour de la donnée. L'ambition est bien de faciliter l'harmonisation des standards techniques des services Cloud afin de faciliter le traitement des données. Ces labels renforceront l'interopérabilité et la réversibilité afin que le partage de données au sein espaces de données soit plus facile. Cela rejoint des initiatives comme l'*European Cloud User Coalition* (ECUC) qui depuis le mois de janvier 2021 rassemble 13 banques européennes qui souhaitent

37 Stratégie d'accélération « Cloud et Verdissement du Numérique » - Volet Cloud | entreprises.gouv.fr

38 Stratégie d'accélération cybersécurité | entreprises.gouv.fr

39 https://fntc-numerique.com/fr/accueil.html

40 FNTC - LES LABELS (fntc-numerique.com)

41 Role of GAIA-X and European data spaces / Hubert Tardieu Chairman of the Board GAIA-X AISBL

établir de nouveaux standards sur le stockage de données. Lancée en 2019 par la Commerzbank en France, l'ECUC souhaite rendre « *les institutions financières européennes plus indépendantes des fournisseurs de Cloud* »[42].

La réalité de l'interopérabilité

En préambule, il est important de rappeler que l'interopérabilité est, dans certains cas, une exigence déjà ancienne ! Prenons par exemple le Référentiel Général d'Interopérabilité (RGI). Il se définit comme « *un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration. Ces recommandations constituent les objectifs à atteindre pour favoriser l'interopérabilité. Elles permettent aux acteurs cherchant à interagir et donc à favoriser l'interopérabilité de leur système d'information, d'aller au-delà de simples arrangements bilatéraux* » Le RGI est défini dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Dans l'article 11 de cette ordonnance, le « *RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publication de ce référentiel sont fixées par décret* »[43] Au niveau européen l'EIF (European Interoperability Framework) s'inscrit dans la volonté de créer un marché unique numérique en Europe. « *Il propose aux administrations publiques 47 recommandations concrètes sur la manière d'améliorer la gouvernance de leurs activités d'interopérabilité, d'établir des relations inter-organisations, de rationaliser les processus de soutien aux services numériques de bout en bout et de veiller à ce que les législations existantes et nouvelles ne compromettent pas les efforts d'interopérabilité* »[44] Ce souci d'interopérabilité doit être renforcé à tous les niveaux.

C'est aussi ce que martèle l'association GAIA-X au sein de ses « *policy rules* » en distinguant : Portabilité et interopérabilité des données : l'interopérabilité des données doit aller plus loin que la portabilité des données, c'est-à-dire que l'harmonisation sémantique des données spécifiques au domaine est le prochain degré d'interopérabilité des données et devrait inclure, entre autres, une gestion normalisée (spécifiques au domaine) pour les jumeaux numériques. Interopérabilité des services et des contrats pour permettre la collaboration des *Cloud Solution Provider* (CSP). Hubert Tardieu soulignait à ce sujet « *Le principal défi technique est généralement le manque d'interopérabilité. Aujourd'hui, une grande partie des données est stockée dans des Clouds publics, dont 70% sont exploités par des fournisseurs américains. Alors que les clients du Cloud gagnent en flexibilité en ce qui concerne leur propre accès aux ressources de calcul et de stockage, ils peuvent faire face à des défis lorsqu'ils partagent des données avec des partenaires de l'écosystème qui utilisent différents fournisseurs de services Cloud. Des problèmes d'interopérabilité existent au niveau de l'infrastructure en raison de protocoles de communication incompatibles et également au niveau des applications en raison d'un manque d'API communes (un défi que PSD2 a aidé à résoudre dans les services financiers). Une façon d'aller de l'avant serait que les fournisseurs de services Cloud se conforment aux politiques communes convenues pour les infrastructures et les applications* ».

"Quand on parle de Cloud, le champ de la confiance se construit sur toute la sphère numérique, donc au-delà de l'infrastructure. Le Cloud a pour objet de réconcilier, sécuriser et pérenniser la donnée mais aussi de l'utiliser dans un environnement technique où chaque brique fonctionnelle apporte un haut niveau de sécurité et un environnement organisationnel, humain respectueux des règles éthiques.
Chez Docaposte nous apportons des services SaaS de confiance hébergés et exposés grâce à nos propres infrastructures au cloud. Nous venons par exemple de lancer une solution de signature électronique à distance sécurisée par L'Identité Numérique La Poste, première identité numérique qualifiée au niveau substantiel eIDAS par l'ANSSI. En tant que prestataire de services de confiance, nous nous attachons à obtenir les labels et certifications qui font référence pour accompagner les parcours numériques des usagers et entreprises."

Xavier Vaccari - Chief Strategy Officer – Cloud & AI – Docaposte.

42 Des banques européennes s'allient contre la puissance du Cloud américain (courrierinternational.com)

43 Référentiel général d'interopérabilité (RGI) | numerique.gouv.fr

44 The New European Interoperability Framework | ISA² (europa.eu)

Une approche de la sécurité multi-facettes

Alignement lois, contrats et standards techniques : un préalable nécessaire à la sécurité

Le Cloud Act, en permettant aux Etats-Unis, dans le cadre d'une enquête pénale, d'accéder à des données stockées à l'étranger sur des serveurs américains sans en informer les utilisateurs, a ouvert une large brèche en matière de protection des données. La portée extraterritoriale de cette législation conjuguée à l'absence de textes européens sur la nécessaire localisation des données et aux faibles alternatives en matière de Cloud ont offert aux américains un accès aux données des entreprises. Dans ce contexte quelle protection juridique des données industrielles et plus largement des infrastructures européennes faut-il mettre en place ? Comment faire face aujourd'hui au flux d'attaques ?

RAPPORT GAUVAIN

Dans son rapport sur la protection des entreprises contre les lois et mesures à portée extraterritoriale en date du 26 juin 2019, le député Raphaël Gauvain évaluait la loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, dite « loi de blocage ». Il soulignait la nécessaire modernisation de cette loi autour de trois axes : Déclaration aux autorités françaises, accompagnement par une administration et durcissement des sanctions. « Contre le Cloud Act, il propose d'étendre le RGPD aux données des personnes morales, ce qui « *permettra de sanctionner les hébergeurs qui transmettraient aux autorités étrangères des données en dehors de l'entraide administrative ou judiciaire*[1] ». Raphaël Gauvain souhaite également l'élaboration d'une doctrine nationale « sur les secrets à protéger », afin d'éviter, à l'avenir, la transmission d'informations sensibles par nos administrations »

1 Le rapport Gauvain sur la protection des entreprises contre les sanctions américaines

> **La seule stratégie de protection ne permettra donc pas à elle seule de faire émerger des champions européens du numérique : nous devons appeler de nos vœux la mise en place d'une véritable politique de compétitivité européenne alliant formation, recherche, attractivité et investissements. A cet égard, au sein de la commission des lois de l'Assemblée Nationale, nous avons d'ores et déjà à l'esprit qu'il nous faut renforcer nos actions à l'aune de cette crise. Le Droit se doit de réguler nos outils numériques dans toutes leurs dimensions : des réseaux sociaux aux réseaux d'entreprises. Cet effort collectif, dont nul ne doute de la nécessité, devra faire l'objet de réflexions approfondies qui supposent que nous repensions nos modes de gouvernance institutionnelle. A l'instar du monde économique, le monde juridique est indiscutablement en train de basculer dans l'ère du numérique : open data, intelligence artificielle, smart contracts, légaltechs"**
>
> Jean-Michel Mis – député de la 2e circonscription de la Loire

L'alignement lois, contrats et standards est la première chose à suivre. Pour cela, il faut en premier lieu vérifier la cohérence des textes entre eux. Prenons par exemple la problématique de la localisation des données. Dans le Règlement du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux de données à caractère non personnel dans l'Union européenne, il est dit aux alinéas 2 et 4 : « *Toutefois, le fonctionnement efficace et efficient du traitement des données et le développement de l'économie des données dans l'Union sont entravés, en particulier, par deux types d'obstacles à la mobilité des données et au marché intérieur : les exigences en matière de localisation des données mises en place par les autorités des États membres et les pratiques menant à une dépendance à l'égard des fournisseurs dans le secteur privé* ».

« *Ces obstacles à la libre circulation des services de traitement des données et à la liberté d'établissement des fournisseurs de services découlent des exigences, dans le droit des États membres, visant à` localiser les données dans une zone géographique ou un territoire précis à des fins de traitement des données. D'autres règles ou pratiques administratives ont un effet équivalent en imposant des exigences spécifiques qui rendent plus difficile le traitement de données en dehors d'une zone géographique ou d'un territoire précis dans l'Union, telles que les exigences d'utiliser des moyens techniques qui sont certifiés ou agréés dans un Etat membre particulier. L'absence de sécurité juridique quant à` la portée des exigences, légitimes ou non, de localisation des données restreint encore le choix offert aux acteurs du marché et au secteur public concernant la localisation du traitement des données. Le présent règlement ne limite en rien la liberté ´des entreprises de conclure des contrats précisant où les données doivent être localisées. Le présent règlement vise simplement à` sauvegarder cette liberté ´en permettant de convenir d'une localisation située en tout lieu de l'Union* ».

Ce texte peut pourtant apparaître en dissonance avec la volonté actuelle de favoriser une localisation des données au sein de l'Union européenne.

Pour se prémunir d'une utilisation des données dans le cadre de l'application du Cloud Act, encore faut-il avoir contractuellement exigé une notification préalable à l'accès aux données. À ces précautions il s'agit ensuite d'ajouter des standards technologiques qui permettent de suivre la donnée tout au long de son cycle de vie : « *Vous devez ici définir quels niveaux de traçabilité vous souhaitez appliquer, quels types de chiffrement pour quels usages* » Adrien Basdevant - Basdevant Avocats, CNNum.

Sur la sécurité de l'IoT, les constats sont identiques : « *Nous devons être plus prescriptifs. L'enjeu de régulation est de taille et aujourd'hui, la discontinuité des normes est un facteur d'insécurité juridique pour les acteurs de l'IoT* » Raphaël de Cormis – Thalès.

OSE

« Un OSE est un opérateur tributaire des réseaux ou systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société. Les obligations s'appliquant aux OSE sont de trois sortes : application de règles de sécurité aux systèmes d'information essentiels (SIE) identifiés par l'OSE ; notification à l'ANSSI des incidents de sécurité survenus sur les SIE ; l'ANSSI, ou un prestataire d'audit qualifié par l'ANSSI, peut contrôler la conformité de l'OSE aux règles de sécurité ainsi que son niveau de sécurité[1] »

1 https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/faq-operateurs-de-services-essentiels-ose/

Le cas particulier des OIV et OSE

OIV, OSE présentent des avantages que le groupe de travail autour de ce livre blanc a souhaité explorer.

En parallèle l'OIV[45] (Opérateur d'Importance Vitale), défini dans le code de la Défense, est en France, une organisation identifiée par l'Etat comme ayant des activités indispensables à la survie de la nation. D'après le SGDSN (Secrétaire Général de la Défense et de la Sécurité Nationale) « *les opérateurs d'importance vitale sont désignés par le ministre coordonnateur du secteur qui les sélectionne parmi ceux qui exploitent ou utilisent des installations indispensables à la vie de la Nation* ». Au cours de la procédure de sélection, une consultation des OIV pressentis avec une concertation interministérielle est réalisée pour protéger de manière équivalente les 12 secteurs d'activités d'importance vitale.
Dans ce contexte, comment faire évoluer les référentiels actuels afin d'inclure la prestation « Cloud » dans les OIV ?

Le soutien apporté par l'ANSSI aux OIV en matière de cybersécurité est important. Elle assure notamment, une fonction de centre de réponse et de traitement des incidents de sécurité (CSIRT).

Les CSIRT qui en font la demande et en obtiennent l'autorisation peuvent utiliser le terme de CERT, signifiant Computer Emergency Response Team dans leur nom.

Notons ici que face à l'augmentation en quantité et en sophistication des attaques informatiques, et à leurs impacts potentiellement destructeurs, « *l'article 22 de la loi de programmation militaire (loi n° 2013-1168 du 18 décembre 2013), qui fait suite aux préconisations du Livre blanc sur la défense et la sécurité nationale de 2013 rajoute une pierre à l'édifice en imposant aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV). Cette sécurisation passe notamment par l'application d'un certain nombre de règles de sécurité. La France est le premier pays à être passé par la réglementation pour mettre en place un dispositif efficace et obligatoire de cybersécurité de ces infrastructures critiques* »[46] Dans la même veine et pour améliorer la compréhension collective de l'internet, un Observatoire de la résilience de l'internet français a été inauguré en 2011 sous l'égide de l'ANSSI.

Dans les propositions faites, les déclinaisons sectorielles des centres d'échange et d'analyse de l'information comme les ISAC(s) seraient une solution. Ils ont pour mission de recueillir, analyser et diffuser des renseignements sur les menaces et doivent fournir à leurs membres des outils pour atténuer les risques et améliorer la résilience des installations. Ancrés dans les secteurs, les ISAC(s) communiquent des informations critiques et maintiennent, à l'échelle du secteur, un bon niveau d'information.[47]

45 https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006182855/
46 Protection des OIV en France | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
47 National Council of ISACs (nationalisacs.org)

CSIRT ET CERT

Créé en 1988 après la propagation d'un « ver internet » qui se répliquait et exploitait diverses failles de sécurité du système Unix, le *Computer Emergency Response Team* (CERT) ou *Computer Security Incident Response Team* (CSIRT) est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.

Les tâches prioritaires d'un CSIRT sont les suivantes :

- Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;
- Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CSIRT, contribution à des études techniques spécifiques ;
- Établissement et maintenance d'une base de données des vulnérabilités ;
- Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incidents ou au pire leurs conséquences ;
- Coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CSIRT nationaux et internationaux.

Source : ssi.gouv.fr

> **Si je ne devais faire qu'une préconisation pour la France ou pour l'Europe, ce serait de décliner la notion d'ISAC ou de CSIRT sectoriel. Il y a quelques exemples, comme France Cyber Maritime"**
>
> Olivier Caleff – Cyber-résilience and CSIRT Security expert

FRANCE CYBER MARITIME[1]

Fin 2019, un groupe de travail, sous le pilotage du Secrétariat Général de la Mer (SGMer) a réuni les premiers acteurs volontaires des secteurs maritime et cyber. Ses travaux permettent de définir l'objet et les missions d'un centre national de coordination de la cybersécurité pour le maritime et de proposer la création d'une structure juridique pour passer de la conception à la réalisation.

L'association loi 1901 France Cyber Maritime voit le jour le 17 novembre 2020, avec le soutien du SGMer, de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et d'une quinzaine de partenaires publics et privés.

Ses missions :

- Encourager le développement d'une filière d'excellence française en cybersécurité maritime, en proposant une offre de services et solutions adaptée aux besoins du secteur ;
- Accroître la résilience du monde maritime et portuaire face aux risques cyber, en créant et mettant en œuvre un Maritime Computer Emergency Response Team.

1 France Cyber Maritime – FRANCE CYBER MARITIME (france-cyber-maritime.eu)

Notons enfin qu'un certain nombre d'initiatives en matière de cybersécurité sont lancées. Le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, aura son siège à Bucarest, en Roumanie. Il sera le principal instrument de l'UE pour coordonner et mettre en commun les investissements sur la cybersécurité[48]. Il fonctionnera séparément de l'ENISA (Agence de l'Union Européenne pour la Cybersécurité) qui aide l'Europe à se préparer aux cyber défis de demain. « Par le partage des connaissances, le renforcement des capacités et la sensibilisation, l'Agence collabore avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, renforcer la résilience des infrastructures de l'Union et, en fin de compte, assurer la sécurité numérique de la société et des citoyens européens[49] »

L'ENISA joue un rôle important auprès des Infrastructure et services essentiels telles que les centrales électriques, les systèmes de transport, les installations de fabrication sont contrôlées et surveillées par les systèmes de contrôle industriel (ICS), y compris les systèmes SCADA (*Supervisory Control and Data Acquisition*). Ses publications sectorielles présentent les défis à relever et dressent un ensemble de solutions. C'est le cas notamment de la conférence ENISA-ERA : « Cybersécurité dans les chemins de fer »[50], de la cartographie des initiatives en matière de cybersécurité du secteur financier au niveau de l'Union Européenne[51] ou des dernières préconisations faites aux directions des achats des hôpitaux[52].

48 Le nouveau Centre européen de compétences en matière de cybersécurité sera situé à Bucarest, en Roumanie. - Consilium (europa.eu)
49 About ENISA - The European Union Agency for Cybersecurity — ENISA (europa.eu)
50 Cybersecurity in Railways Conference: Key Takeaways — ENISA (europa.eu)
51 EU Cybersecurity Initiatives in the Finance Sector — ENISA (europa.eu)
52 Procurement Guidelines for Cybersecurity in Hospitals: New Online tool for a Customised Experience! — ENISA (europa.eu)

C'est en clarifiant le rôle de ces différents acteurs et en favorisant les échanges avec les entreprises nationales que, collectivement, nous serons en mesure de limiter les impacts des cyberattaques. Les cinq vœux formulés par le groupement Hexatrust et le Club des directeurs de sécurité des entreprises (CDSE) en association avec le Club des juristes, vont dans ce sens et militent pour un renversement de la tendance actuelle afin d'établir un équilibre en matière d'autonomie numérique, en bâtissant une alternative européenne à la concurrence mondiale. Ils proposent un plan d'équipement cyber et de continuité d'activité numérique, l'instauration d'une proportion d'achats fléchés vers les PME françaises de confiance, la constitution d'une Europe de la cyber, un financement conséquent des ETI de croissance et le développement d'une « Couverture Assurantielle du Cyber-Risque » qui permettrait aussi d'étendre la garantie responsabilité civile professionnelle et la garantie perte d'exploitation aux aspects cyber face à la multiplication des risques de droit européen[53].

Tour d'horizon des solutions et commentaires

La création d'un Cloud de confiance doit être accompagnée d'outils techniques assurant la sécurité des données hébergées afin que les entreprises aient confiance dans l'infrastructure et y hébergent leurs données. Concernant la sécurité, trois éléments sont importants : le chiffrement, l'authentification et le contrôle permanent des accès à la donnée et ceci au-delà des incidents.

Le chiffrement des données peut-il être considéré comme une réponse fiable et si oui dans quel cadre ? Le chiffrement par quorum n'est-il pas trop complexe pour être accessible techniquement par un grand nombre d'entreprises ? Quelles sont les autres solutions à envisager ?

Trois constats proposés par François Desnoyer – Safran LS – viennent poser le cadre de cette réflexion :

« *Le chiffrement des données est un moyen de sécurisation qui ne peut être considéré comme une réponse absolue à tous les types de menaces. Selon que l'on souhaite se protéger des hébergeurs, d'attaques internes ou d'attaques externes, les moyens de sécurisation doivent faire l'objet de stratégies différenciées.*

Le chiffrement ne peut par ailleurs pas être considéré comme un moyen suffisant pour les entreprises pour se protéger d'une préemption et d'une exploitation des données par des États malveillants.

L'usage du chiffrement constitue donc à ce jour pour l'entreprise une réponse partielle pour : protéger le transport de données, se protéger des hébergeurs et répondre à des exigences normatives ou réglementaires ».

« *Notons toutefois que le chiffrement peut être réalisé sur les processeurs eux-mêmes* » note Raphaël de Cormis – VP Thalès Digital Factory. C'est

53 P5 vœux pour mener une politique prioritaire de l'industrie du numérique en France et en Europe – HEXATRUST

ce que les Enclaves sécurisées explorent. Ainsi un processus peut créer une enclave sécurisée dans la mémoire. Les données enregistrées au niveau de cet espace mémoire sécurisé ne sont déchiffrées qu'au sein du processeur et suivant des instructions exécutées depuis l'enclave elle-même. Le surcoût d'une telle solution doit être évalué. Ce type de réponse est à l'étude dans certaines entreprises.

Google Cloud a sur ce sujet présenté deux solutions, *Assured Workloads et Confidential VM*[54], pour apporter davantage de chiffrement de données et restreindre les emplacements de stockage à une localisation particulière. Ceci concerne en priorité les entreprises régulées et les agences gouvernementales.

Dans l'utilisation du chiffrement comme moyen de protection contre l'hébergeur, le problème est celui de la gestion des clés qui ne peut être confiée à l'hébergeur et doit se faire du côté du client.

Deux possibilités pour cela, côté client :

- Centraliser la gestion des clés dans un HSM (*Hardware Security Module*) : avantage = centralisation et facilité de gestion, possibilité de stopper le déchiffrement à tout moment du fait de l'architecture centralisée, inconvénient = risque de déchiffrement sur une requête de l'hébergeur illégitime et difficulté à discerner les requêtes hébergeurs légitimes des non-légitimes, points de vulnérabilité lors du déchiffrement en RAM ou pendant le transport.
- Embarquer les clés sur les stations des utilisateurs (clé personnelle pour chaque utilisateur directement sur le poste de travail) : avantage = déchiffrement au plus près de l'utilisation, moins de points de vulnérabilité dans la chaîne complète de traitement de la donnée. Inconvénient : Des solutions de marché existent mais restent onéreuses et lourdes à déployer.

Cette deuxième solution qui semble à privilégier du point de vue de la sécurité peut s'avérer chère et complexe à mettre en œuvre, et ne pas adresser par ailleurs totalement la diversité des cas d'utilisations sur les postes utilisateurs. Elle ne répond en effet pas notamment au besoin croissant de traitements et de calcul sur les données en temps réel du fait des nouveaux besoins et de l'émergence de nouvelles architectures de traitement de l'information davantage orientées évènement que transaction.

Les solutions de chiffrement présentent donc des limites aux cas d'utilisation actuels des entreprises. Pour augmenter le niveau global de sécurisation des informations et des infrastructures, plutôt que de renforcer les moyens de chiffrement, il paraît davantage utile de travailler à :

- Augmenter le niveau de confiance sur l'hébergement par un meilleur encadrement réglementaire des activités des hébergeurs, notamment pour ce qui concerne l'encadrement de leurs personnels qui n'est pas uniformément réglementée et qui constitue un point de vulnérabilité, La France se place quant à elle à un bon niveau d'exigence.
- Renforcer les mécanismes d'authentification à tous les étages des transactions (vérifier les demandes et les autorisations d'accès)
- Développer des concepts autour de la blockchain appliqués à l'identité. « *Elles s'appuient sur le principe qu'à partir du moment où il n'y pas de base de données centrale, (un hébergeur qui détiendrait l'ensemble des données chiffrées, cryptées) mais que les données sont réparties chez les utilisateurs, c'est-à-dire détenues en propre par les wallets des utilisateurs. Le risque d'attaque est alors quasi nul. Il serait nécessaire d'attaquer tous les porteurs de wallets individuellement, ce qui reste bien plus complexe et donc plus long et visible* » Olivier Senot – Docaposte

CLÉ DE DÉCHIFFREMENT : TUERIE DE SAN BERNARDINO LE 2 DÉCEMBRE 2015

Deux tireurs ouvrent le feu dans un centre destiné à accueillir des personnes au chômage ou sans-abris. Pour les besoins de l'enquête, le FBI demande à Apple de débloquer l'Iphone d'un des suspects, mort pendant l'attaque, afin d'exploiter les informations qu'il contenait. La multinationale refuse d'aider les enquêteurs à accéder au contenu chiffré de l'appareil.

Apple, par le design de son produit, n'était pas capable de révéler la clé de déchiffrement. Le FBI devait en théorie utiliser une méthode dite de « force brute » permettant de tester toutes les combinaisons possibles de codes secrets pour pouvoir déverrouiller le téléphone. C'est pourquoi le FBI a judiciairement ordonné à Apple de créer un outil logiciel permettant de débloquer sa propre sécurité informatique. Si l'agence fédérale a finalement réussi à déverrouiller l'iPhone sans l'aide constructeur, plusieurs procédures sont aujourd'hui en cours aux États-Unis pour accéder aux contenus chiffrés des téléphones dans d'autres affaires similaires[1].

1 AWS KMS : y a t-il vraiment un intérêt à importer ses propres clés de chiffrement ?

Ce sujet s'est transformé en droit français par la limitation des clés de chiffrement utilisables par le civil.

Une des solutions pour avoir une garantie de neutralité serait qu'un tiers de confiance suffisamment neutre (et ce terme reste à définir) pourrait garder des clés. « *Dans le cadre d'une utilisation par des terroristes quel que soit le motif, une procédure judiciaire demanderait via ce tiers de confiance l'ouverture des conversations. Un des moyens de la garantie de neutralité, serait que cet acteur central qui détiendrait les clés (ce serait un single point of failure) pourrait être régi par les notions de quorum. Si plusieurs acteurs doivent être d'accord pour ouvrir les clés sur un chiffrement par quorum alors le tiers de confiance neutre n'a accès à rien. Nous pourrions aller vers des clés à 2048 ou 4096 (très grosses clés qui donnent des garanties techniques) et une procédure légalement encadrée qui nécessite l'accord des parties concernées par les données incriminées* » Olivier Senot – Docaposte

Une harmonisation des contraintes réglementaires au niveau européen portant sur les hébergeurs avec des policy rules (du type de GAIA-X) strictes seraient de nature à renforcer le niveau de confiance sur le fait que l'hébergeur serait davantage responsabilisé et serait auditable et

54 https://www.cloudanalogy.com/news/google-cloud-introduces-confidential-vms-and-assured-workloads/

> “GAIA-X est un écosystème numérique réglementé par ses membres. L’initiative vise à créer un environnement dans lequel les données peuvent être partagées et stockées sous le contrôle des propriétaires et des utilisateurs de données ; et où les règles sont définies et respectées, afin que les données et les services puissent être rendus facilement disponibles, compilés et échangés.”
>
> Olivier Senot – Docaposte

contrôlable sur la manière de traiter nos données. Cela permettrait de diminuer le risque de fuite de données du fait de l’hébergeur.

L’émergence de GAIA-X, de règles adaptées, et d’un contexte réglementaire européen harmonisé permettra d’initier une convergence des acteurs vers une nouvelle façon d’opérer le Cloud et d’augmenter le niveau de confiance des entreprises sur l’hébergement.

Les solutions de chiffrement par quorum semblent un complément séduisant mais restent à ce stade à l’état de théorie et ne semblent pas encore supportées par des solutions de marché. Quant à la conteneurisation, elle semble être un outil davantage intéressant pour favoriser l’interopérabilité et la réversibilité des déploiements d’applicatifs sur les Clouds plutôt qu’un dispositif de sécurisation à part entière. C’est un levier intéressant pour gérer la réversibilité, faciliter le changement d’hébergeur et diminuer la dépendance à celui-ci.

Pourtant, en matière d’authentification sur la provenance de la donnée nous pouvons créer des conteneurs et suivre la vie des conteneurs, on assure alors une certaine intégrité. « *Ce sont des choses qui débutent. Ce qui existe est le cryptage de bout en bout. C’est le cryptage SSL. Mais les attaques par l’intérieur ne sont pas robustes à ce type de protection. Les chiffrements en 4096 ont un coût en puissance de calcul. Si vous devez encrypter un flux de caméra en 4K (10 000 caméras pour la ville de Paris) cela devient problématique. Faut-il tout sécuriser ? On pourrait nativement ou en programmation indiquer que certaines données sont critiques ou non* » Olivier Senot – Docaposte.

« *L’authentification pose des problèmes spécifiques au déploiement des technologies de l’usine 4.0 avec le déploiement d’IoT dans les usines et la robotisation des procédures. Nous sommes très prudents sur ce point et découplons bien sûr nos différents réseaux pour garantir la sécurité. Ce peuvent être des découplages logiques traités par une architecture réseau spécifique ou une rupture de la continuité numérique lors de l’introduction d’une étape de validation par un utilisateur réel dans un processus transactionnel entre un robot et SAP par exemple* ». François Desnoyer – Safran Landing Systems.

Stratégie d’accélération cyber : les actions en cours

Cloud de confiance, cybersécurité de confiance, autant de termes qui vont dans le sens d’une meilleure compréhension des enjeux de protection des données par la filière numérique :

« *La cybersécurité est le pilier fondamental sans lequel ne peut se mettre en place et prospérer une économie numérique. Elle est un enjeu stratégique aujourd’hui selon trois dimensions : sécuritaire-de souveraineté, sociétale et économique. L’activité numérique de nos économies devient une composante de notre compétitivité et de notre capacité à relever les défis du futur qu’ils soient technologiques ou organisationnels. Pour une bonne gouvernance de la confiance et de la sécurité, l’un des facteurs à prendre en compte est aussi la notion de dépendance, cet environnement de confiance doit répondre, au-delà de la sécurité à l’impératif pour les utilisateurs de ne pas être techniquement dépendant d’une infrastructure pouvant « couper » le service au nom d’une décision externe au pays concerné.* » Olivier Senot – Docaposte.

L’objectif assigné à l’horizon 2025 à la stratégie nationale d’accélération cyber, est l’atteinte d’un chiffre d’affaires de 25 Md€ pour la filière (soit un triplement du chiffre d’affaires actuel), le doublement des emplois dans le secteur en passant de 37 000 à 75 000 emplois et l’émergence de trois licornes françaises en cybersécurité. Sur la page du Ministère de l’Économie des Finances et de la Relance dédiée à ce sujet[55], il est rappelé les cinq priorités de cette stratégie qui s’articulent avec le travail de régulation mené par la CNIL :

- Développer des solutions souveraines et innovantes de cybersécurité ;
- Renforcer les liens et synergies entre les acteurs de la filière ;
- Soutenir la demande (individus, entreprises, collectivités et Etat), notamment en sensibilisant mieux tout en faisant la promotion des offres nationales ;
- Former plus de jeunes et professionnels aux métiers de la cybersécurité, fortement en déséquilibre ;
- Soutien en fonds propres.

Une petite dizaine d’actions concrètes sont déjà listées. On retrouve, entre autres, un appel à projets (AAP) visant à soutenir le développement de briques technologiques critiques (2021/2022), le renforcement du niveau de sécurité de l’Etat (2021/2022), Un appel à manifestation d’intérêt (AMI) pour « Sécuriser les territoires », la mise en place d’une journée « autonomie et sécurité numérique » (2021) ou encore le soutien aux projets du Campus Cyber (2021/2022)[56].

Adoptée par les institutions européenne le 6 juillet 2016 la directive Network and Information (NIS) doit permettre d’assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d’information de l’Union européenne. Elle vise à « *l’émergence d’une Europe forte et de confiance, qui s’appuie sur les capacités nationales des Etats membres en matière de cybersécurité, la mise en place d’une coopération efficace et la protection des activités économiques et sociétales critiques de la nation, pour faire face collectivement aux risques de cyberattaques* »[57].

La directrive MIS a été « un outil privilégié pour accélérer le développement d’un écosystème de confiance ». Elle est aujourd’hui en phase de révision afin de faire face à des menaces différentes selon les secteurs « *Dans ce contexte, il est primordial que NIS constitue le cadre législatif européen de référence en matière de cybersécurité, reposant sur un dispositif d’harmonisation minimale et de portée transversale* »[58].

---

55 Stratégie d’accélération cybersécurité | entreprises.gouv.fr
56 Stratégie d’accélération cybersécurité | entreprises.gouv.fr
57 https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/
58 https://www.ssi.gouv.fr/actualite/revision-de-la-directive-nis-une-opportunite-pour-renforcer-le-niveau-de-cybersecurite-au-sein-de-lue/

Les garanties de réversibilité / les principes de transversalité

Dans les débats sous-jacents au Cloud de confiance, la question de la réversibilité – capacité d'un client à changer de fournisseur de services Cloud – se pose avec force. D'une part, les conditions qui poussent un client à choisir un fournisseur Cloud à un instant T peuvent évoluer, et, d'autre part, dans le cas d'un marché public, la mise en concurrence régulière est presque obligatoire.

Si plusieurs acteurs se partagent le marché du Cloud, au premier rang desquels les hyperscalers américains, force est de constater que la mobilité inter-Cloud ou la migration d'un environnement Cloud vers un environnement *on-premise*[59] restent difficiles en termes de coût et de temps. Les échanges autour de ce livre blanc ont fait émerger les notions « *d'irréversibilité* » des choix, et de nécessité de se « sevrer » des solutions packagées présentes sur le marché. Au terme de réversibilité les participants ont préféré celui de « transversalité » d'un fournisseur de Cloud à un autre.

Des solutions techniques à ne pas négliger

Plusieurs solutions techniques permettant le transfert de données d'un Cloud public à un environnement on-premise existent :

- Les fournisseurs de Cloud proposent eux-mêmes des solutions propriétaires dont les coûts sont souvent prohibitifs

- Il est possible d'installer des logiciels marché tel que la licence Vmware, dont l'installation doit être effectuée à la fois chez le client et chez le fournisseur Cloud.

La réversibilité a donc un double coût financier et temporel. Pour résoudre ce frein essentiel, la voie réglementaire pourrait jouer un rôle important en contraignant les offres de Cloud à faciliter le transfert de données et à le rendre plus fluide. Néanmoins, une solution de ce type au niveau européen nécessite du temps pour aboutir ; s'il ne faut pas exclure ce chemin, un autre est envisageable.

Mutualiser les investissements entre plusieurs sociétés concernant les solutions de rapatriement de données

La problématique de transfert de données (réversibilité ou mobilité concurrentielle) s'impose à tous les clients de Cloud. En mutualisant les investissements sur les infrastructures qui permettent de transférer les données d'un Cloud public à un environnement on-premise, par exemple vers des solutions marché telle que la licence Vmware, les entreprises pourraient voir le coût de transfert baisser tout en obtenant un meilleur délai commercial. Cet investissement commun sur une capacité technique permettant de se détacher d'un Cloud semble intéressant pour favoriser encore un peu plus la concurrence.

De cette autonomie technologique nous retiendrons en priorité la nécessité d'une compréhension fine de l'ensemble des acteurs de la chaîne du Cloud, d'un renforcement de la position des tiers de confiance, d'une plus grande coordination des travaux transverses en matière de cybersécurité et de promotion d'un encadrement européen qui intègre l'ANSSI et L'ENISA. Enfin, les travaux menés sur le Edge Computing en vue de leur transfert vers des acteurs européens clés devront être, eux aussi, renforcés.

59 on-premise = environnement informatique de l'entreprise en français

> « Au terme de réversibilité nous préférons celui de "transférabilité" d'un fournisseur de Cloud à un autre »
>
> Jérôme Martin – BearingPoint System Security

AUTONOMIE DÉCISIONNELLE

« L'autonomie stratégique c'est la somme de trois libertés : liberté d'appréciation, liberté de décision et liberté d'action » Livre blanc sur la défense et la sécurité nationale de 2008

L'Union Européenne, autour du DGA, vise à penser la liberté de circulation des données, opposant ainsi un modèle alternatif à la centralisation et la captation des données par les plateformes. Le numérique européen, human centric et non pas platform centric, est un numérique où l'internaute recouvre pleinement son pouvoir de décision. Plus on partage les données, plus on échappe au phénomène d'enfermement des écosystèmes logués, et plus on irrigue celui des écosystèmes ouverts. Le Cloud européen, en permettant la compatibilité des plateformes par défaut au profit des parties prenantes de son territoire et en facilitant la portabilité des données entre les personnes, devient une clef de voûte de cette stratégie européenne de la donnée.

La question que nous nous posons ici est donc la suivante : comment organiser cette circulation des données pour retrouver nos marges de manœuvre décisionnelles ? Et comment un Cloud de confiance peut y aider ?

Sept axes structurent ce que nous regroupons dans l'autonomie décisionnelle du Cloud de confiance :

- Inciter au partage ;
- Renforcer la coopération par filière ;
- Encourager une plus grande transparence dans les contrats ;
- Clarifier le champ des compétences réglementaires du tiers de confiance ;
- Identifier les actions de concurrence déloyale et notamment les ventes liées ;
- Appuyer les engagements visant à conforter notre autonomie stratégique par un lobbying approprié ;
- Renforcer les critères environnementaux dans les appels d'offres.

Inciter au partage

La Commission européenne a dévoilé fin 2020, plusieurs projets de règlements dont le *Data Governance Act* (DGA) prévoyant une gouvernance européenne des données. Qu'en est-il exactement et comment s'inscrire dans son sillage ?

Huit chapitres structurent le règlement autour de notions de réutilisation des données, d'accroissement de la confiance et d'altruisme des données. La plaquette mise en ligne[60] insiste sur la valeur économique du partage des données et propose la mise en place d'un « *European Data Innovation Board* » qui aura la charge du pilotage de la gouvernance et qui veillera à hiérarchiser les standards.

60 Data Governance Act | Shaping Europe's digital future (europa.eu)

Renforcer la coopération par filière

Les initiatives poussées par le Comité Stratégique de Filière (CSF) des industries de la sécurité

La mission est de faire émerger des acteurs Cloud dits « de confiance » pour le IaaS, le PaaS et le SaaS, tout en favorisant la filière française. Pour atteindre cet objectif, deux axes sont explorés : la sécurité des données et l'indépendance numérique. Dans une interview récente Edouard de Rémur – Oodrive – apportait des précisions importantes à la définition d'un Cloud de confiance : « *Au sein du CSF nous avons souhaité positionner le Cloud de confiance sur deux piliers principaux : d'une part, un tiers de confiance, l'ANSSI, qui valide la partie sécurité et d'autre part, la vérification que le capital du CSP est à 51% européen. Des critères d'auditabilité, de réversibilité et d'interopérabilité viennent compléter cette définition* ».

Il renvoie aux travaux menés par le CIGREF ces derniers mois et notamment une phase de tests et de validations de solutions en réponse à des cas d'usage proposés par les entreprises. L'objet est de valider la pertinence et la réactivité de l'offre de la filière industrielle nationale.

Fonctionnement des espaces de données sectoriels et gouvernance

Prenons ici la structure de GAIA-X :

- Le premier niveau consiste, en fédérant les fournisseurs européens de Cloud, à disposer de ressources techniques et technologiques à même d'offrir des services Cloud compétitifs. Les « policy rules », socle de règles et de principes édictés par le consortium, doivent être ratifiées par les entreprises souhaitant rejoindre Gaia-X qui fournira un label en fonction des caractéristiques des services offerts.

- Le second niveau concerne les espaces de données sectoriels. Ils permettront d'entraîner les différents moteurs technologiques, qu'il s'agisse des méthodes d'apprentissage profond (« deep learning » en anglais) ou d'intelligence artificielle (IA). Ces espaces de données sectoriels visent à rassembler des acteurs économiques évoluant sur une même verticale afin qu'ils puissent, sur leur périmètre, échanger des données.

Si les investissements vers des solutions de gestion de données sont devenus essentiels pour les entreprises, les stratégies d'échange de données constituent un enjeu d'avenir. Pour une entreprise, rejoindre un espace de données dans le cadre d'un Cloud de confiance européen signifie, d'une part, un accès à une banque de données plus importante que celles disponibles en interne, et d'autre part, un fonctionnement respectueux de la législation européenne.

Comme nous venons de l'énoncer, la gouvernance générale du projet GAIA-X est régie par le socle de règles et de principes édictées dans le document « policy rules ». Néanmoins, la relation interentreprises au sein des dataspaces n'obéit pas aux mêmes logiques. Effectivement, les dataspaces sont autonomes dans leur fonctionnement et la notion d'enveloppe juridique pour les régir ne semble pas avoir été soulevée par le Cloud de confiance. En l'absence de structure juridique établie pour encadrer les relations interentreprises au sein d'un dataspace, la coopération s'exercera de pair à pair, entre les parties-prenantes elles-mêmes.

L'intérêt principal des dataspaces, c'est la réunion d'acteurs d'un même secteur autour d'un intérêt de filière. Dans leur fonctionnement, chaque dataspace profitera du caractère moteur d'un acteur en particulier, chargé d'organiser la collaboration avec d'autres entreprises du secteur. A titre d'exemple, c'est la Caisse des Dépôts et Consignations, une institution financière publique française, qui endosse actuellement le rôle de « préfigurateur » du dataspace finance au sein du Cloud de confiance. L'acteur qui joue ce rôle au sein d'un data space doit ainsi proposer, par le biais de groupes de travail avec les parties-prenantes, une organisation qui doit réunir un consensus. Néanmoins, l'intérêt de filière dépassera-t-il les intérêts individuels des entreprises participantes ?

La première des propositions serait d'introduire une notion de « tiers de confiance » ou « d'arbitrage » pour chaque espace de données sectoriel du Cloud de confiance. Ce tiers serait finalement le garant de l'intérêt de filière au sein de chaque espace de données sectoriel.

Les acteurs du domaine de la santé ont intérêt à partager des données pour faire avancer la recherche en médecine, par exemple, ou encore pour améliorer la pertinence des diagnostics ou l'accès aux parcours de soins. Les données médicales revêtent donc un enjeu majeur. Il faut donc réussir à ce que toutes les parties-prenantes partagent leurs données et s'arranger pour que la recherche effectuée à partir de ces datasets primaire et secondaire soit partagée entre tous. La présence d'un tiers de confiance concernant l'organisation d'un espace de données sectoriel pourrait justement permettre d'éviter tous problèmes. Une chose reste sûre : chaque secteur fait face à des problématiques distinctes, et le domaine de la santé, par son caractère essentiel, sera clé pour démocratiser les usages dans d'autres secteurs.

L'échange de données au sein des espaces de données sectoriels

Au niveau européen, il existe différentes typologies en fonction du partage de données ; deux scénarios se distinguent :

Le partage de données BtoG[61] est régulé : l'échange de données entre une entité publique et une entité privée est régi par des obligations de mise à disposition de données de l'Etat à certaines entreprises, ou dans certains secteurs spécifiques comme la mobilité, d'ouverture de données des entreprises à l'Etat. A titre d'exemple, les grands fournisseurs d'énergie ont l'obligation d'ouvrir aux gouvernements leurs bases d'adresses, sans contreparties ou négociations.

Le partage de données BtoB[62] s'autorégule : l'échange de données entre entreprises privées s'organise à partir de recommandations de partage. La réglementation européenne sur les données industrielles étant à ses débuts, « *la structuration et les obligations concernant le partage de données business se feront par les pratiques contractuelles entre les acteur*s ».

S'agissant de la sphère des données personnelles, nous disposons d'une longue expérience avec, d'une part la création d'autorités administratives au sein des États membres depuis 40 ans, et d'autre part, la mise en œuvre, en 1995, de la directive européenne 95/46/CE « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données »[63]. S'agissant des données privées, industrielles, la régulation se structure actuellement ; nous sommes ainsi dans une forme d'autonomie des acteurs à travers des mécanismes d'autorégulation.

61 BtoG est l'abréviation anglaise de Business to Government (de l'entreprise vers l'Etat)

62 BtoB est l'abréviation anglaise de Business to Business (d'une entreprise vers une autre entreprise)

63 https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:31995L0046

Néanmoins, force est de constater que sur le Cloud de confiance s'échangeront des données personnelles et non personnelles. En cas de litige, quelle réponse envisager au sein d'un dataspace ? Est-ce au *Comité européen de la protection des données* ou aux autorités administratives concernées des États membres de statuer sur les questions de données au sens large du terme ? Doit-on mettre sur pied une autorité administrative indépendante européenne dédiée aux données non-personnelles ?

En France, la *Commission nationale de l'informatique et des libertés* (CNIL) est l'autorité administrative indépendante dédiée à la question des données à caractère personnel, émettant des avis non-normatifs.
Si un litige est constaté dans un data space dont le préfigurateur est français, est-ce à la CNIL, à l'*Autorité de la concurrence*, à l'ARCEP ou encore au *Conseil Supérieur de l'Audiovisuel* de se prononcer ?

Dans les propositions soulevées, il y a la nécessité de réfléchir, au sein des instances organisationnelles du Cloud de confiance, aux manières d'empêcher des litiges / de statuer si un litige se produit au sein d'un dataspace.

Tous les scénarios doivent être envisagés pour permettre la réussite du Cloud de confiance. S'il ne faut pas inhiber totalement les bonnes pratiques de coopération dans des règles, le risque étant de sacrifier le pragmatisme sur l'autel de la conformité, la question mérite d'être traitée.

Encourager une plus grande transparence dans les contrats

L'efficacité d'un Cloud repose sur la standardisation et la mutualisation des ressources. Au-delà des exigences imposées ces derniers mois par l'Europe, le contrat signé avec le prestataire de Cloud constitue un enjeu important. Une attention particulière doit être portée aux clauses relatives a :

- La mise en place de mesures de sécurité idoines : liste des mesures techniques et organisationnelles garantissant la sécurité des traitements selon l'article 32 et 40 (mise en place d'un code de conduite) du RGPD ;
- À l'encadrement des transferts de données hors de l'UE et au respect des exigences du référentiel SecNumCloud[64] ;
- Aux déclarations relatives à la sous-traitance (Articles 28, 30.2 et 37 du règlement européen sur les obligations du sous-traitant)[65] ;
- À l'exercice du droit d'audit (application des procédures SOC (*Service Organisation Control*) en matière de gestion des risques ;
- Aux conditions de réversibilité et de portabilité (telles que définies à l'article 20 du RGPD)[66] ;
- À l'indication claire du cadre réglementaire. Nous avions précédemment soulevé l'importance d'une signature du contrat en droit français ;
- Des précisions sur la « territorialisation » du stockage et de l'opération des données ;

L'arrêt Schrems II rendu le 16 juillet 2020 a invalidé la décision de la Commission européenne relative à l'adéquation de la protection des données personnelles assurée par le Privacy Shield. Cet arrêt a pour conséquence immédiate d'interdire les transferts de données à caractère personnel vers les États-Unis sur la base du Privacy Shield. Dans ce contexte, le principe d'accountability se pose plus que jamais. Selon la Cnil, il « *désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données* »[67]. Des garanties complémentaires de différentes natures (contractuelles, organisationnelles ou techniques) doivent être prévues et comporter des possibilités de contrôle sur pièces ou sur site.

64 secnumcloud_referentiel_v3.1_anssi.pdf
65 RGPD - Guide sous-traitant (cnil.fr)
66 Professionnels : comment répondre à une demande de droit à la portabilité ? | CNIL
67 https://www.cnil.fr/fr/definition/accountability

Clarifier le champ des compétences réglementaires du tiers de confiance

Nous avons exploré précédemment la notion de tiers de confiance. Il est ici intéressant de mettre en lumière les compétences réglementaires dont ce tiers de confiance peut bénéficier. Cette approche conduit à reconnaître que le tiers de confiance vérifie un certain nombre d'exigences en matière de souveraineté, à commencer par la localisation des données.

Une autre alternative concerne la fiducie de données (cf. encadré). Un livre blanc consacré à ce sujet étudie comment les fiducies de données peuvent aider l'industrie « *à aller au-delà de la simple conformité aux règles de protection de la vie privée, pour renforcer la confiance du public* ».[68] Le document étudie l'application des modèles de fiducie de données à trois cas d'utilisation – données urbaines, données médicales et données issues des plateformes en ligne – pour en faire ressortir les enjeux qui restent à approfondir.

FIDUCIE DE DONNÉES

La problématique du tiers de confiance a donné lieu en décembre 2018 à un atelier international organisé par un fournisseur de produits en IA (Element AI) et une fondation pour l'innovation (Nesta), dans l'objectif d'évaluer la fiducie de données en tant que solution pour renforcer juridiquement la protection des données des individus.

D'après l'Open Data Institute :

« *Une fiducie de données doit disposer d'un objectif clair ; d'une structure juridique et d'une constitution légale ; de fiduciaires ; de certains droits et obligations sur les données gérées ; d'une description du mode de répartition des bénéfices ; d'un financement durable* ».

Dans ce cadre, les données sont confiées à des tiers de confiance (fiduciaire, ou trustee) par l'entreprise ou la plateforme (le constituant) au profit d'un bénéficiaire, l'internaute.

D'après les auteurs, ce modèle fiduciaire offrirait « *une grande flexibilité, car les modalités de la fiducie peuvent être taillées sur mesure en fonction d'un ensemble de données, d'un problème ou d'un objectif donné* ».

Le Livre Blanc propose ainsi le modèle d'une règlementation d'anticipation face aux transformations rapides impulsées par le numérique, où la fiducie de données porterait en elle une dimension d'inclusivité et de collaboration, une attitude prospective et une approche « expérimentale proactive » pour favoriser l'innovation.

Source : https ://hello.elementai.com/rs/024-OAQ-547/images/Fiducies_de_Donnees_FR_201914.pdf

68 Fiducies de Données Un nouvel outil pour la gouvernance des données

Identifier les actions de concurrence déloyale et notamment les *ventes liées*

Dans les préconisations soulevées, le cas des ventes liées est apparu comme une action, qui dans le cadre des offres des *hyperscalers*, pouvait conduire à une forme de concurrence déloyale. En subordonnant l'achat d'un service à l'achat d'autres services, certains fournisseurs de Cloud entravent la vente de services connexes par des entreprises concurrentes. Ces pratiques rendent opaque l'offre à partir du moment où chaque service vendu ne bénéficie pas d'un prix associé.

Des obligations en matière de vente subordonnée ou dite conjointe pourraient être édictées à commencer par une lecture individualisée des services et de leurs prix, compris dans un package. Ceci permettrait aux entreprises de choisir ou non l'ensemble de l'offre en bénéficiant de tarifs modulaires.

Appuyer les engagements visant à conforter notre autonomie stratégique par un lobbying approprié

Le constat largement partagé ressort des différents entretiens : la difficulté à mettre en place des actions de lobbying suffisantes qui permettraient de faire entendre des avis contradictoires auprès des instances européennes concernées par le Cloud. Aujourd'hui, force est de constater que les budgets alloués au lobbying sont encore trop faibles au regard des actions menées par des fournisseurs de Cloud étrangers. La création d'une cellule de lobbying partagée pourrait s'avérer utile.

Des actions de communication vers les PME peuvent être mises en place notamment via le contrat de filière. L'industrie française de sécurité rassemble aujourd'hui un nombre important d'ETI, de PME et de startups dynamiques et innovantes sur tout le territoire. Le Comité stratégique de filière poursuit différents enjeux de compétitivité et de souveraineté. Les signataires ont fixé cinq projets ambitieux de natures très différentes : la sécurité des grands évènements et des JO Paris 2024, la cybersécurité et la sécurité de l'Internet des objets, l'identité numérique, les territoires de confiance et le numérique de confiance qui doit permettre à une offre de Cloud de confiance compétitive de se déployer.

Deux points sont intéressants ici à retenir et à valoriser :

- Ce comité stratégique de filière rassemble et se fait porte-parole des « *principales entreprises industrielles et de service de la filière, les groupements industriels (ACN, l'AN2V, la FIEEC, le GICAT, le GICAN, HEXATRUST), les organisations syndicales de salariés, des représentants des pôles de compétitivités de la filière, des représentants des collectivités locales, ainsi que les représentants de l'État et des établissements publics les plus directement investis dans le soutien de la filière des industries de sécurité ». Ils rappellent que les régions ont un rôle important à jouer dans des projets structurants comme le fait d'assurer « le développement d'une compétence régionale adaptée aux spécificités du tissu industriel, des bassins d'emplois et des orientations de politique industrielle et d'innovation de chaque région* »

- Le choix de grands projets pour expérimenter à grande échelle les capacités de nos forces de sécurité. « *A cet égard, les Jeux Olympiques et Paralympiques représentent un évènement sportif et de société, mondial et hors norme, d'une visibilité et d'un impact inégalés, sur une durée qui va bien au-delà de celle des Jeux eux-mêmes. En tant que nation hôte, réussir les JOP, sur tous les plans, est à la fois un impératif et une opportunité exceptionnelle de valoriser le savoir-faire et la marque France, en mettant en avant des premières en termes d'usages et de technologies …La sécurité des grands évènements, qu'ils soient sportifs (JO, mondiaux, etc.), culturels (grands concerts), diplomatiques (G7, G20), ou autres, est un thème particulier qui nécessite de mettre en œuvre un ensemble de capacités (contrôle d'accès, gestion des flux, coordination des forces, cybersécurité, etc.) avec des niveaux de performance élevés, sans dégrader l'expérience des participants. De plus, ces capacités doivent, dans la mesure du possible, s'intégrer avec d'autres activités spécifiques de l'événement (billetterie, applications, broadcast, etc.) comme aux activités générales qu'elles soient d'ordre régalien ou privé (visa, transport, hôtellerie, etc.) Les technologies à maîtriser pour y exceller sont nombreuses (biométrie, vidéo intelligente, IA, détecteurs, communications, coordination à la demande, etc.). C'est un domaine en forte croissance sur lequel les attentes sont de plus en plus conséquentes et que la filière souhaite soutenir en y apportant une offre structurée* »[69].

D'autres projets comme le Grand Paris Express peuvent être l'occasion de proposer des concessions de service où les données des différents acteurs présents pourront être croisées afin de participer au développement de villes intelligentes. C'est ce que Marie-Christine Servant – Responsable de l'Unité numérique de la Société du Grand Paris, appelle de ses vœux « *A titre d'exemple, les informations sur les flux des voyageurs peuvent si elles sont partagées avec l'écosystème autour d'une gare permettre aux commerces locaux d'optimiser le dimensionnement de leurs ressources ou valoriser de façon plus pertinente la publicité en gare ou à l'extérieur. Elles peuvent également permettre de dimensionner de façon prospective les infrastructures urbaines dans les projets d'aménagement. Le Wifi est un générateur d'information sur les flux ou les files d'attente à l'intérieur des gares qui peuvent se déporter sur les territoires et inversement. (Ex. file d'attente devant les distributeurs bancaires). Des données issues de capteurs de luminosité des parvis des gares peuvent permettre également de mieux gérer l'éclairage urbain et d'améliorer la sécurité aux abords des gares. On peut aussi songer à des formes de mutualisation entre des prestataires en gare et à l'extérieur de la gare (ex pour les handicapés). La valeur est souvent générée par le croisement entre plusieurs sources de données : certaines données du GPE croisées avec des données territoriales pourront vraisemblablement permettre de créer de nouveaux services* ».

69 https://www.conseil-national-industrie.gouv.fr/files_cni/files/csf/Securite/contrat_csf_industries_de_securite_janvier_2020.pdf

Renforcer les critères environnementaux dans les appels d'offres notamment

Quelques chiffres en introduction permettent de mesurer l'importance d'une approche environnementale et de son introduction dans les appels d'offres. « D'ici 2030, les Data Centers du monde entier pourraient engloutir 10% de la production mondiale d'électricité contre déjà 3% à l'heure actuelle. Aujourd'hui, les Data Centers représentent à eux seuls 17% de l'empreinte carbone de la technologie »[70]. Quels sont, dans ce contexte, les apports du Green Cloud Computing et quelles solutions différenciantes pouvons-nous proposer ? Comment faire de cette approche un levier de compétitivité ?

Les apports du Green Cloud Computing ou verdissement numérique

Le Green Cloud Computing est un terme désignant le fait de réduire l'empreinte environnementale du *Cloud Computing*. Cette empreinte prend en compte la consommation énergétique, mais aussi les déchets matériels, les types de matériaux utilisés et l'économie de toutes autres ressources (électricité, eau, etc.). Il existe différentes méthodes de calcul afin d'évaluer l'empreinte environnementale.

Les techniques utilisées par les *data centers* pour réduire l'empreinte environnementale sont à la fois matérielles (processeurs moins gourmands en énergie, bâtiments plus performants, évacuation de la chaleur) mais aussi logicielles (algorithme de réduction de consommation, utilisation de la virtualisation)[71].

Incorporer dans les SLA (Service Level Agreement) traditionnels des clauses « green » permet au client de vérifier que le service acheté respecte un certain niveau de qualités environnementales. Ceci était déjà annoncé

70 Comment réduire l'impact des Data Centers sur l'environnement (lebigdata.fr)
71 Green Cloud Computing — Wikipédia (wikipedia.org)

et développé dans un article de 2017 « Exploiting Renewable Sources: When Green SLA Becomes a Possible Reality in Cloud Computing »[72].

Intégrer des clauses de recycling / upcycling

Ces clauses de recyclage ou de surcyclage (le produit issu du recyclage a plus de valeur que le produit initial) peuvent être prévues dans les contrats. Elles concernent notamment des pièces d'équipement devenues obsolètes. Ainsi les ventilateurs ou processeurs peuvent être démontés et vendus sur plusieurs marchés. Le cuivre, l'acier et l'aluminium trouvent eux aussi des voies d'utilisation nouvelles bien que la liste des composants réutilisables ne soit pas encore complètement claire.

Le développement de l'*upcycling* pose la question du nettoyage des données sensibles. Que faut-il conserver et à quel moment dans la chaîne de retraitement des déchets ? Quelles sont les garanties proposées par les acteurs de l'*upcycling* ?

Obliger les entreprises à justifier leur choix de Cloud

En annexe des appels d'offres une grille d'analyse permettrait de définir chaque solution, ses avantages et ses conséquences en matière d'impact environnemental. Il ne s'agit pas ici d'obliger les entreprises à choisir la solution à empreinte carbone faible mais bien de donner à réfléchir afin que les décisions soient arbitrées au mieux. Ainsi, aujourd'hui, il existe des premières analyses mesurant l'empreinte carbone d'installations : on premise, virtualisée (Cloud privé), en Cloud public ou sans serveurs (*serverless computing*). Dans ce dernier cas, le fournisseur de serveur gère dynamiquement les ressources allouées au service client.

72 Exploiting Renewable Sources: When Green SLA Becomes a Possible Reality in Cloud Computing | IEEE Journals & Magazine | IEEE Xplore

> **D'autres initiatives existent comme cette école Green IT[1]. qui rassemblera fin juin 2021, les meilleurs experts scientifiques reconnus dans le domaine du numérique responsable, du Green IT, de l'énergie (matérielle et logicielle), des data centers et du Cloud"**
>
> Adrien Lèbre – IMT Atlantique

1 GREEN IT numérique responsable : 28 juin-2 juil. 21 - Formation - Université de Pau et des Pays de l'Adour (UPPA) (univ-pau.fr)

AUTONOMIE PÉDAGOGIQUE

« La souveraineté éducative c'est pouvoir résister au solutionnisme numérique des GAFA. » Marie-Christine Levet dans le rapport « Préserver notre souveraineté éducative » publié par Digital New Deal en 2019.

La souveraineté numérique se joue aussi sur le terrain des compétences et de la formation

L'ingénierie des solutions n'est pas visible, et mal comprise : l'importance de la culture numérique pour analyser, décoder et critiquer

L'acquisition et l'entretien des compétences constituent deux sujets critiques pour concevoir et opérer un système d'information dans le Cloud – partiellement ou totalement – tout en étant capable d'intégrer les évolutions technologiques continues concernant le traitement, le stockage, le calcul des données et la sécurisation. En effet, des ressources humaines et/ou matérielles sont nécessaires aux directeurs de systèmes d'information (DSI) pour piloter efficacement leur transformation.

Pourtant, comme en témoigne François Desnoyer, *Chief Digital et data Officer chez Safran Landing Systems, « les populations de techniciens se sont appauvries au fil des années* ». Les DSI des industriels du numérique manquent ainsi de ressources compétentes pour s'occuper, de manière proactive, de la transformation numérique de l'entreprise.

Le développement du *self-learning* : les DSI face au développement croissant de l'expertise des métiers, opportunité plus que menace

Une dynamique semble néanmoins exister au sein des équipes métiers ; la montée en compétences sur les nouvelles technologies progresse. L'utilisation standard du langage de programmation Python, à titre d'exemple, dépasse désormais le cadre des bureaux d'étude. Également, le recours à des Cloud publics pour supporter le traitement de données non-sensibles permet aux équipes métiers de renforcer leurs compétences en termes de nouvelles technologies. Il n'est ainsi pas rare de constater que les équipes métiers disposent de davantage de compétences sur ces nouveaux environnements, en nombre et en niveau, que certaines équipes DSI.

Si cette dynamique d'autoformation doit être encouragée tant elle apparaît bénéfique pour l'entreprise – sensibilisation des équipes métiers aux enjeux data et amélioration de la capacité à résoudre des problèmes aux plus près des utilisateurs – elle est toutefois inégale. Le succès de l'autoformation, renforcé notamment par le contexte sanitaire actuel et les périodes successives de télétravail, a mis en lumière l'impuissance des directions informatiques centrales face à la montée en compétences des équipes métiers. Si les DSI ne sont pas réfractaires à ces démarches individuelles, elles s'interrogent néanmoins sur la manière de les rationaliser et de les organiser : comment coordonner une démarche de formation des équipes centrales et métiers d'un groupe industriel du numérique à l'échelle internationale et auprès de milliers d'employés ?

En effet, cet environnement hétérogène de formation présente plusieurs limites :

- Rupture de la continuité numérique entre les informations du système d'information legacy et les traitements de données dans les Cloud publics amenés à les utiliser, et inversement
- Risques pour la sécurité avec l'augmentation de la surface d'exposition à des cyberattaques
- Création de dépendances à des éditeurs de technologies et perte de maîtrise de nos schémas directeurs

La mondialisation du marché des compétences Cloud et data et la généralisation du travail à distance : offshorer n'a jamais été aussi facile

Faut-il évoquer ici aussi la question des politiques d'achats des entreprises (qu'elles soient du numérique ou non) et qui structurent de nouvelles dépendances : exemple : externalisation à forte dose de développements informatiques vers des pays *low cost*. Avec pour conséquence une forme de glissement des compétences : préemption assumée par Facebook de développeurs où qu'ils se trouvent sur la planète sans avoir besoin de leur

attribuer un bureau dans la Silicon Valley, et transfert de développements informatiques de nos multinationales vers l'Inde par exemple.

Une offre de contenus de formation préemptée par les *hyperscalers* : un accès difficile à un contenu de formation neutre et indépendant

HYPERSCALERS : DES RÉALITÉS DIFFÉRENTES SELON LES PAYS

Les hyperscalers sont les industriels leaders du Cloud public qui utilisent l'architecture Hyperscale pour leurs Data Centers. Cette architecture « *désigne des systèmes de Cloud Computing évolutifs dans lesquels un très grand nombre de serveurs sont reliés ensemble au sein d'un réseau. Le nombre de serveurs utilisés peut être revu à la hausse ou à la baisse en fonction des besoins. Un réseau de ce type peut traiter un très grand nombre d'accès, mais aussi mettre à disposition des capacités plus restreintes en cas d'utilisation faible* ».

Autrement dit, les hyperscalers ont une capacité d'adaptation en temps réel et à l'agilité malgré leur taille colossale. Il est intéressant de souligner à l'inverse que la traduction française de « gros hébergeurs » ne traduit pas cette idée d'agilité, puisque l'hébergement de données suggère leur mise à l'abri dans une structure statique, peu adaptable.

Cette nuance sémantique est assez symptomatique des différences entre les Etats-Unis et la France. D'un côté, une promesse de scalabilité et d'innovation, de l'autre une promesse d'extensibilité et d'immobilité ...

Source : https ://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-lhyperscale/

Un système en tension, des acteurs sous pression

Ces grands acteurs ont déployé une stratégie politique et commerciale de formation efficace, qui s'organise de plusieurs façons :

Les étudiants soumis à la pression de l'employabilité : se former aux outils Google et Amazon est un plus

Une influence auprès des écoles : à l'instar de l'éditeur américain MathWorks qui a distribué des licences gratuites dans les écoles d'ingénieurs et les universités pour ensuite pénétrer les bureaux d'étude en entreprise, les grands acteurs du numérique fournissent également les écoles et universités avec des conditions d'accès préférentielles à leurs services.

Les académiques soumis à une double pression : la demande des étudiants, et la contrainte économique pour produire des contenus et accéder à des ressources indépendantes

Une stratégie progressive « d'enfermement » sur leurs contenus de formation qui réplique le modèle des plateformes B2C : les contenus basiques de formation sont d'abord accessibles gratuitement dans une logique de modèle freemium, les ressources de formation deviennent alors payantes de manière graduelle. Les parcours certifiants délivrés par ces acteurs disposent aujourd'hui d'une valeur parfois plus importante que des certifications académiques. L'effet « lock-in » sur lequel repose le succès des plateformes numériques de services grand public fonctionne ainsi également sur les contenus de formation.

Les startups soumises à un impératif de passage à l'échelle et de time to market : les standards d'hypercroissance utilisés par les investisseurs guident les choix techniques vers les offres des hyperscalers

Une influence auprès des startups et incubateurs : de la même manière, les grands acteurs du numérique distribuent leurs solutions dans des écosystèmes d'innovations technologiques, à titre d'exemple un incubateur comme Station F[73].

Les points d'accès à la formation sur les environnements Cloud et IA sont également contrôlés. Deux éléments concourent à cela : d'une part, Google profite de la domination internationale de son moteur de recherche, et d'autre part, l'abandon en 2018 par Google de sa philosophie de « PageRanking » agnostique a conduit à la résurgence de contenus sponsorisés et d'offres commerciales. Les démarches de formation ou

73 Start, Grow, Scale with Google @Station F - Accueil

d'autoformation utilisant le moteur de recherche de Google semblent donc irrémédiablement servir les intérêts de la firme américaine

Les grandes et moyennes entreprises sous la pression de la rentabilité et de la continuité du service rendu : le choix des économies d'échelle

Enfin, il convient d'envisager la capacité de lobbying et d'influence des géants du numérique au niveau européen ; l'exemple le plus récent étant le document confidentiel du groupe américain Google pour « contrer Thierry Breton »[74] et ses ambitions sur le paquet législatif *Digital Services Act* – un projet de régulation des plateformes Internet.

74 Digital Services Act : Thierry Breton obtient des excuses du patron de Google

Des propositions pour le développement d'une autonomie pédagogique

Pour favoriser, d'une part, la montée en compétences des acteurs industriels et des entreprises, et assurer, d'autre part, une meilleure indépendance vis-à-vis des plateformes, il apparaît primordial de mener une action sur les contenus de formation.

Le renforcement de la culture numérique des décideurs

Si un grand nombre de ressources existent pour former les collaborateurs des entreprises, de manière organisée ou via l'autoformation, il faut faciliter l'accès à des ressources objectives – c'est-à-dire indépendantes des enjeux commerciaux des plateformes – afin de proposer une alternative effective aux programmes de formation en ligne proposés par les *hyperscalers* tels que Google Cloud ou Amazon Web Services.

- Création d'un dispositif d'accompagnement spécifique : décoder, décider ? (Format innovant à définir pour favoriser une parole décomplexée)

- Création du manifeste du décideur agile (dans l'esprit du manifeste agile -> quelques CEO volontaires co producteurs/signataires d'une charte management/décision 4.0) ? Contenu intégré aux programmes de formation dirigeants (MBA, MBA corporates)

Favoriser/ aider la production de contenu indépendant

- Prise en charge par l'État des coûts de production de contenus pédagogiques indépendants, coproduits entre académiques et entreprises et disponibles en libre accès. Des initiatives comme le service public PIX, pour évaluer, développer et certifier ses compétences Cloud sont intéressantes. Le matériel pédagogique mis à disposition est complet et permet à l'enseignant/ administrateur de préparer les contenus et les épreuves[75] .

Le pari de la mutualisation

L'intérêt d'associer les entreprises et les universités dans une démarche de mutualisation des moyens de formation réside chez les nouvelles générations. Ce sont elles qui seront amenées à utiliser des solutions Cloud à l'avenir ; les former est donc primordial pour l'avenir de l'autonomie stratégique européenne.

Ces contenus de formation mutualisés pourraient adresser deux enjeux en priorités : d'une part, des cursus techniques informatiques (IT), et d'autre part, des cursus orientés sur la gestion des risques IT (comprendre les stratégies technologiques propriétaires et d'enfermement propriétaire, construire une stratégie fournisseur, comprendre les enjeux d'autonomie stratégique et l'environnement actuel de guerre économique...).

- Subvention par l'Etat de la production de contenus de formation co produits entre entreprises

Développer et installer une nouvelle certification technique Cloud

- Création d'un parcours agnostique, certifiant, pour le développement de compétences professionnelles de conception et mise en œuvre de solutions Cloud et data, référence pour grands groupes et ETI et valeur d'employabilité pour étudiants. Les 2 priorités : architecture, et développement (-> *code is law, architecture is politics*) ;

- Avec une introduction de la culture numérique au sens géopolitique ;

- Une ouverture à l'ensemble du territoire national et aux acteurs internationaux du domaine (Campus cyber et formation de l'ANSSI).

75 https://pix.fr

LE CAMPUS CYBER

Initié par le président de la République, le Campus Cyber sera à l'horizon 2021 un lieu clé de la cybersécurité qui regroupera les principaux acteurs nationaux et internationaux du domaine. Il accueillera sur un même site des entreprises (grands groupes, PME), des services de l'Etat, des organismes de formation, des chercheurs et des associations. À ce jour, plus de 60 acteurs issus de multiples secteurs ont indiqué leur volonté de participer au Campus.

Convaincu que l'écosystème cyber est le levier pour accélérer la création d'une société numérique de confiance, et fondé sur des valeurs d'excellence, de confiance et de partage, le Campus Cyber veut promouvoir une filière d'excellence française en cybersécurité, fédérer les talents dans un lieu commun autour de projets innovants, et développer les communs de la sécurité et de la confiance numérique.

Source : https ://www.ssi.gouv.fr/uploads/2019/10/leaflet-campus.pdf

L'offre de service « Parcours de cybersécurité » est proposée par l'ANSSI aux collectivités territoriales et aux organisations au service des citoyens dans le cadre de France Relance.

Dans un post d'avril 2021, Guillaume Poupard, Directeur Général de l'ANSSI en définit les contours « *Son objectif ? Élever le niveau de sécurité des systèmes d'information de ses bénéficiaires via la mise en œuvre de parcours de sécurité adaptés aux enjeux et aux besoins des organisations. L'accompagnement des bénéficiaires est le maître-mot de cette offre de service*[76] »

- Architecture : principes Cloud / on premise, interopérabilité, sécurité, ...

- Développement : devops, conteneurisation, ...

- Créer le TOEIC du Cloud

  - Imposé par les entreprises à ses personnels et sous-traitants ;

  - Implication des directions achat (intégration aux contrats des gros intégrateurs pour formation des personnels en retour) ;

  - Critères d'embauche sur les postes Cloud et CTO.

76 https://www.ssi.gouv.fr/agence/cybersecurite/le-volet-cybersecurite-de-france-relance/securiser-le-socle-numerique-de-letat-des-collectivites-territoriales-et-des-organismes-au-service-des-citoyens/les-parcours-de-cybersecurite/

CONCLUSION

Ce livre blanc a pour objectif de répondre à certaines grandes questions, souvent très concrètes, que se posent les entreprises sur la protection de leurs données sensibles et des traitements associés, dans un contexte géopolitique, juridique, technique, et commercial que beaucoup jugent instable et donc dangereux.

Tous nos échanges se sont orientés vers la construction de propositions pragmatiques et économiquement viables, permettant une meilleure appropriation des enjeux du Cloud par les grands groupes.

En apportant ces éclairages, nous aspirons à accompagner le travail structurant des organisations tels que l'ANSSI qui participent activement à la création des conditions d'un « Cloud de confiance », et avons souhaité contribuer à la définition d'une autonomie stratégique que nous appelons tous de nos vœux.

En structurant nos réflexions sur les autonomies technologique, décisionnelle et pédagogique, nous avons voulu finalement répondre directement à l'ambition de la Mission Numérique des Grands Groupes qui consiste faire accéder à notre économie un nouveau palier de transformation numérique.

Le Cloud est en effet au fondement de ces questions puisqu'il est le préalable à l'émergence d'un écosystème autour de la souveraineté des données, et le socle sur lequel nous pouvons développer une stratégie commune sur l'intelligence artificielle.

« *Le stockage et le traitement des données est un enjeu de souveraineté pour les décennies à venir. Mais pour que les données soient stockées et traitées à l'européenne, en conformité avec des standards et des valeurs européens, le plus simple est encore d'européaniser les GAFAM* »
André Loesekrug-Pietri, Jean-Hervé Lorenzi, Thierry Vandewalle dans Le Grand Continent[77].

77 https://legrandcontinent.eu/fr/2021/03/23/souverainete-numerique-etre-audacieux-europeaniser-les-gafam/

Finalement, ce livre blanc aura tenté de s'inscrire dans la double ambition d'un cloud souverain européen.

D'une part, protéger nos entreprises de situations de monopoles qui provoquent des dépendances mortifères. C'est notamment le cas de nos propositions qui tendent à sécuriser le marché.

D'autre part, promouvoir nos intérêts en offrant les conditions de création d'une offre alternative aux hyperscalers chinois et surtout américains. Ce qui passe par la promotion de standards garants de nos valeurs européennes et humanistes.

L'Europe peut, notamment via Gaïa-X, faciliter une européanisation des hyperscalers sur son territoire, mais aussi demain ailleurs dans le monde en attirant petit à petit ces grandes plateformes dans sa toile. A l'instar du RGPD qui est devenu de facto une norme mondialisée, le cloud de confiance européen peut imposer sa vision d'un internet des Lumières. Ouvert, décentralisé et écologiquement responsable.

Gageons que le cloud européen devienne ainsi le terreau de cette « Green Silicon Valley » que Thierry Breton et Ursula Von Der Leyen appellent de leurs vœux.

Annexe : lettre de mission

Mission Numérique des Grands Groupes

MINISTÈRE
DE L'ÉCONOMIE
DES FINANCES
ET DE LA RELANCE

Liberté
Égalité
Fraternité

COMMUNIQUÉ DE PRESSE

Lancement de la mission numérique des grands groupes

Paris, le 5 Août 2020
N°77

L'accélération de la transformation numérique des entreprises est un enjeu majeur pour assurer la compétitivité de notre économie. Pour y répondre, **une mobilisation collective est devenue indispensable** et l'Etat souhaite donner l'impulsion nécessaire pour faire de la France un leader en la matière.

Dans ce contexte, **Bruno Le Maire**, ministre de l'Economie, des Finances et de la Relance, **Agnès Pannier-Runacher**, ministre déléguée à l'Industrie, et **Cédric O**, secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques, officialisent **la création de la mission numérique des grands groupes**, dont Juliette de Maupeou (vice-présidente Innovation & Stratégie, Capgemini Invent) et Nicolas Guérin (digital experience Officer, Natixis), sont nommés coordonnateurs. La Direction Générale des Entreprises (DGE) apporte son appui à cette mission.

Fruit de la **mobilisation d'un large groupe de grandes entreprises françaises**, tous secteurs d'activités confondus, ainsi que de l'ensemble des acteurs économiques et sociaux concernés, cette mission vise à faire émerger des projets communs et concrets, qui bénéficieront à l'ensemble du tissu économique français, avec l'ambition de le faire accéder à un nouveau palier de transformation numérique, dont la crise a révélé l'urgente nécessité.

Les réflexions engagées s'articuleront autour de 5 grands chantiers identifiés comme prioritaires :

1. soutenir la transformation des compétences et des formations ;
2. accompagner l'émergence d'un écosystème autour de la souveraineté des données au niveau européen ;
3. simplifier et renforcer la collaboration entre start-ups et grands groupes ;
4. participer à la protection de notre souveraineté en matière d'e-paiement ;
5. développer une stratégie commune sur l'intelligence artificielle.

Chaque chantier établira un diagnostic des freins et opportunités liés et formulera préconisations et orientations sur les projets et investissements à envisager. Le cas échéant, **l'Etat pourra soutenir la mise en œuvre des mesures concrètes et projets collectifs qui émergeront de cette mobilisation dans le contexte de la relance.**

Le **comité de pilotage de la mission numérique des grands groupes se réunira pour un premier point d'étape à l'automne. Lors de cette session, les pilotes de chaque chantier présenteront l'état d'avancement des travaux débutés en mars,** les grandes orientations prises et les premiers projets engagés ou à lancer, avec un objectif de livraison, dans la mesure du possible, fixé avant fin 2021.

Cabinet de Bruno Le Maire
01 53 18 41 13
presse.mineco@cabinets.finances.gouv.fr

Cabinet d'Agnès Pannier-Runacher
01 53 18 44 38
presse.semef@cabinets.finances.gouv.fr

Cabinet de Cédric O
01 53 18 43 10
presse@numerique.gouv.fr

139, rue de Bercy
75012 Paris

Annexe : organisation et composition de la mission numérique des grands groupes

Pilotes de la mission :

- Nicolas Guérin (NATIXIS) ;
- Juliette de Maupeou (CAPGEMINI INVENT).

Pilotes des chantiers :

- **Chantier Cloud Européen :** Laurence Houdeville (BEARING POINT) / Laurent Maumet (SOITEC) / Nicolas Guy (SOYHUCE)
- **Chantier Formation / Compétences :** Sophie Marot-Rémy (Euler Hermes – Groupe Allianz) / Nicolas Pauthier (L'OREAL)
- **Chantier Relations Grands Groupes / Start-ups :** Maud Funaro (E. LECLERC) / Thibault Viort (ACCORHOTELS) / Charles Thomas (COMET)
- **Chantier Data / IA :**
  - **Data :** Meriem Riadi (SUEZ) / David Lépicier (PERNOD RICARD)
  - **IA :** Nozha Boujemaa (MEDIAN TECHNOLOGIES) / Samir Amellal (LA REDOUTE)
- **Chantier e-paiement :** Marie Even (C DISCOUNT) / Alexandre Albarel (WORLDLINE)

Comité de pilotage :

Outre les pilotes de chantiers, sont membres du comité de pilotage :

- Nicolas Guérin (NATIXIS) ;
- Juliette de Maupeou (CAP GEMINI INVENT) ;
- Luc Barnaud (NATIXIS) ;
- François Gauthier (VEOLIA) ;
- Mathias Vicherat (DANONE) ;
- Yves Tyrode (BPCE) ;
- Sylvia Métayer (SODEXO) ;
- Marko Erman (THALES) ;
- Henri Pidault (SNCF) ;
- Vincent Colegrave (SOLVAY).