Le cloud de confiance

LIVRE BLANC

CERTIGNA by tessi

Sommaire

Introduction

Selon une étude Gartner, 28 % des dépenses informatiques des entreprises dans le monde seront consacrées au cloud d'ici 2022, contre 19 % en 2018. Si l'usage du cloud est en constante progression depuis une dizaine d'années, le marché mondial a récemment pris une nouvelle ampleur : représentant 45,3 milliards de dollars en 2017, le marché du cloud pourrait atteindre 278,3 milliards de dollars en 2021[1]. Pour les entreprises, le cloud est principalement synonyme de scalabilité, vitesse et agilité, avantages qui font écho à la nécessaire adéquation aux nouveaux usages numériques et à la capacité des organisations à se maintenir dans l'innovation.

Pour une très grande part, cet appel au cloud s'explique par la crise du covid-19 et la nécessité de recourir massivement aux outils collaboratifs en ligne, d'e-commerce, de formation à distance et de diffusion de contenus en continu, indispensables à la continuité de l'activité.

28 % DES DÉPENSES INFORMATIQUES DES ENTREPRISES SERONT CONSACRÉES AU CLOUD D'ICI 2022, CONTRE 19 % EN 2018

Ainsi, la moitié des entreprises prévoient de transférer d'ici deux ans l'ensemble de leurs données vers le cloud. Pour autant, comme le montrent de récentes études[2], les entreprises s'inquiètent de la sécurité des données qui y sont stockées, que le cloud soit public ou privé. En France, en 2012, une première tentative de sécurisation des données avait été initiée par la création de Numergy et Cloudwatt, clouds concurrents financés par des industriels français avec le soutien de l'État. Ces clouds dits « souverains » avaient pour vocation de protéger les données sensibles des entreprises et de l'administration françaises, tout en offrant une alternative aux services américains – ultradominants sur le marché. Si ces deux initiatives sont considérées comme des échecs commerciaux, il n'en demeure pas moins qu'**un besoin fort de confidentialité et de sécurité des données hébergées dans le cloud subsiste.** Depuis le 25 mai 2018 et l'application du règlement européen général sur la protection des données (RGPD), les entreprises se doivent d'être beaucoup plus vigilantes dans leurs choix en matière de cloud computing. Outre la non-conformité au RGPD, d'autres risques pèsent sur les entreprises, tenues d'assurer la protection de leurs données, notamment sensibles : parmi les principaux risques identifiés, le Cloud Act signé par les États-Unis en 2018 ou encore l'espionnage industriel en provenance de pays tiers.

[1] Selon une étude Gartner, Inc. "Predicts 2020: Negotiate Software and Cloud Contracts to Manage Marketplace Growth and Reduce Legacy Costs." December 18, 2019

[2] Selon une étude Oracle et KPMG : https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf et le Livre blanc AFNOR « Cybersécurité et Confiance numérique »

Cloud de confiance, l'avenir du cloud ?

Quelle serait votre définition du cloud souverain et du cloud de confiance ?

Je ne ferai pas de grandes différences. Disons que pour dépasser les nuances de vocabulaire qui visent à faire oublier les ratés des projets de cloud souverains trop franco-français de 2012, le cloud souverain renvoie l'utilisateur – le client – à la souveraineté du contrôle sur ses données et le rassure avec la localisation de leur stockage sur le territoire national. Dans ce cas, la souveraineté vise à sécuriser le client par la localisation. C'est surtout une question d'affichage.

Quant au cloud de confiance, la notion est plus large et renvoie non pas exclusivement à la localisation du stockage sur un territoire donné ou à l'exclusivité des opérateurs mais plutôt à l'impossibilité d'intrusion de puissances étrangères ou malveillantes. Cela peut passer par des acteurs – des briques – qui peuvent être non nationales.

Dans les deux cas, l'État français va chaperonner la contractualisation avec le fournisseur de cloud qui propose une « mise à l'abri des données » mais dans le premier cas elle reposera sur la localisation (où sont-elles stockées ?) et dans le second cas sur les intervenants (par qui sont-elles stockées ?).

Dans tous les cas, l'État en général et le ministère de l'Économie en particulier interviennent techniquement, juridiquement et même d'un point de vue organisationnel, soit en créant ex nihilo les briques du cloud souverain – et nous nous souvenons des échecs de Numergy et de Cloudwhat – soit en agrégeant celles qui existent et fonctionnent déjà – OVH, Outscales, etc.

La question centrale est majeure : c'est celle de la protection de nos données, donc de nos entreprises, contre des intrusions étrangères malveillantes mais aussi contre des sanctions – je pense aux menaces du Cloud Act américain – qui seraient incongrues et coûteuses !

À quels enjeux répond ce cloud souverain ou de confiance ?

Bien sûr dans un monde de plus en plus globalisé, il y a des contraintes de volumétrie, de réactivité et d'interopérabilité à traiter donc il y a des enjeux techniques et informatiques. Mais ce sont avant tout des enjeux juridiques et réglementaires qui pilotent ces projets. Il s'agit en priorité de traiter la question de la sécurité d'hébergement des données mais aussi la responsabilité – du client, du fournisseur, de l'État – en cas de dysfonctionnement du cloud, de vol, d'altération ou de pertes de données, d'intrusion dans le dispositif.

Concrètement, on en revient au client final et à l'utilisateur – celui qui paie – car en cas de perte de données, par exemple, et dans le cadre de données contractuellement hébergées en France, le client peut se retourner contre son fournisseur auprès d'un tribunal français.

C'est beaucoup plus compliqué si l'hébergement est contracté à l'autre bout de la planète.

Et puis il y a bien sûr la dimension diplomatique, liée à l'implication des États que j'évoquais. La position des États européens et de la France sur la protection des données personnelles et des données des affaires n'a rien à voir avec celle des autres grands acteurs du cloud computing. Je pense bien sûr à la position américaine avec son Cloud Act et les risques de poursuite qu'il fait courir – lutte contre le terrorisme oblige – aux entreprises françaises qui hébergeraient leurs données via les solutions de Amazon, IBM ou Google. Des négociations sont en cours pour lever ou alléger cette menace et je pense qu'elles vont réussir tant que 1) les opérateurs américains sont pragmatiques et 2) les acteurs français sont demandeurs ! Le cloud de confiance français intégrera les GAFA !

Ce n'est pas plus mal d'ailleurs car cela va obliger les entreprises clientes à trier et hiérarchiser leurs données avant leur envol vers le nuage…

Après l'échec des premières tentatives de mise en place d'un cloud souverain par la France, quelles sont, selon vous, les chances de succès des nouveaux projets ?

Les États n'ont pas le choix. Il faut que ces initiatives, comme Gaia-X porté par l'Allemagne et la France – avec EDF et Safran notamment – soient menées à bien. Il faut proposer une alternative européenne aux géants du secteur américain et bientôt chinois.

Ce type d'infrastructure est attendu pour sécuriser le climat des affaires et pas uniquement dans les secteurs publics et parapubliques ciblés par le cloud de confiance. La plupart des entreprises et des collectivités ne sont pas conscientes des obligations réglementaires qu'elles ont en termes de collecte, stockage et exploitation de données qu'elles soient personnelles (RGPD) ou professionnelles.

Dès lors, il paraît bien normal de les aider à la fois en les informant et surtout en mettant à leur disposition des infrastructures installées en France et/ou en Europe afin d'être à la hauteur de nos propres exigences de protection.

Pour ces raisons, l'État français a affirmé en 2019 sa volonté de bâtir un « **Cloud de confiance** », qui fait désormais l'objet d'un contrat conclu entre l'État et les acteurs français de la cybersécurité et du cloud, organisés en comité stratégique de filière (CSF). Le cloud de confiance est destiné à héberger les données les plus sensibles, issues des entreprises ou de l'administration, au sein de data centers français ou européens uniquement soumis à la loi française ou européenne. Néanmoins, pour garantir une totale confidentialité des données, **le cloud de confiance doit s'entendre comme un écosystème de français répondant aux normes européennes, dépassant la seule localisation physique des données.**

Le cloud de confiance, une réponse à la multiplication des cyber-risques

En 2019, 65 % des entreprises ont été victimes d'au moins une cyberattaque[3]. 40 % d'entre elles ont même été confrontées à une hausse du nombre de ces attaques par rapport à 2018. Le secteur public n'est pas épargné et constitue également une cible privilégiée pour les hackers. Ainsi, près de 90 % des organisations du secteur public rapportaient avoir été la cible d'au moins une cyberattaque ayant causé des dégâts en 2017 et 2018[4].

D'ici 2021, on estime qu'au niveau mondial, la cybercriminalité aura coûté 6 000 milliards de dollars par an[5]. Un risque d'autant plus grand que la plupart des entreprises et des administrations sont inconscientes des tentatives permanentes d'intrusion dont elles sont la cible de la part de « bots », des robots cyber-pirates à la recherche de la moindre faille dans leur système.

La cybercriminalité touche tous les domaines d'activité : au palmarès des secteurs les plus impactés, les sciences et techniques, le commerce, la finance, l'administration publique[6].

Simples ou complexes, ces attaques peuvent être le fait d'individus isolés, de structures criminelles organisées, de concurrents, ou encore d'organisations étatiques tierces.
Elles ont pour vocation la déstabilisation d'une entité (divulgations de données, prises de contrôle), la recherche d'un profit (en utilisant notamment les techniques du rançongiciel, ou ransomware, et de l'hameçonnage, dit aussi phishing), ou l'espionnage. Dans tous les cas, au-delà du préjudice financier subi, dû par exemple à l'indisponibilité des données, s'en suit toujours une atteinte à la réputation de l'organisme visé.

[3] Selon la 5e édition du baromètre annuel du CESIN : analyse exclusive de la cybersécurité des grandes entreprises françaises
https://www.globalsecuritymag.fr/IMG/pdf/BJ20433_-_Barometre_du_CESIN_vague_5_-Vdef.pdf

[4] Selon une étude Tenable « Cybersecurity in Public Sector: Five Insights You Need to Know »

[5] Selon le « Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac »

6 Selon le baromètre FIC 2020 : https://www.forum-fic.com/Data/DO/tgBloc/23625/fr/params/file/data-breach-long.pdf

Près de 9 entreprises sur 10 utilisent désormais le cloud computing et la popularité grandissante de cette technologie encourage naturellement la multiplication des cyber-attaques.

Entre janvier et avril 2020, les cyberattaques sur les services cloud ont augmenté de 630 %[7], profitant de la fragmentation de la sécurité des systèmes d'entreprise due au télétravail.

Si l'on interroge les entreprises, les cyber-risques seraient principalement liés à une absence de maîtrise de la chaîne de sous-traitance de l'hébergeur, à une non-maîtrise de l'utilisation du cloud par les salariés, et à la difficulté de mener des audits[8]. Pour autant, selon une étude McAfee récente, 79 % des entreprises stockeraient des données sensibles sur un cloud public, représentant au total 26 % des fichiers[9].

9 entreprises sur 10

utilisent le cloud computing

↗ 630 %

L'augmentation du nombre de cyberattaques sur le cloud entre janvier et avril 2020[7]

[7] Selon le rapport Mcafee « COVID-19 Threat Report: July 2020 »

[8] Selon la 5e édition du baromètre annuel du CESIN : analyse exclusive de la cybersécurité des grandes entreprises françaises

[9] Selon le rapport Mcafee « Enterprise Supernova: The Data Dispersion Cloud Adoption and Risk Report », janvier 2020

INTERVIEW DE WAFA BOUAYNAYA, MAÎTRE DE CONFÉRENCES EN SCIENCES DE GESTION, INSTITUT D'ADMINISTRATION DES ENTREPRISES (IAE), UNIVERSITÉ DE PICARDIE

Les dangers du cloud pour les entreprises

Quels sont les principaux risques que fait peser le cloud sur les entreprises ?

J'identifie des risques de trois natures différentes. Tout d'abord, les risques techniques qui touchent à la confidentialité, la disponibilité ou l'intégrité des données externalisées. Concrètement, le cloud computing n'expose pas l'entreprise à des nouveaux risques techniques. Il existe un transfert du risque vers le fournisseur cloud. Que les données des entreprises soient hébergées en interne ou externalisées, le niveau de risque est à peu près équivalent. La seule différence est que dans le cas de l'hébergement sur le cloud, la responsabilité en cas d'attaque ou de perte de données est partagée entre l'entreprise et son prestataire de cloud.

Il existe aussi des risques organisationnels. Par exemple, le manque de compétences internes pour gérer le cloud : de nombreuses PME et ETI ne disposent pas d'un DSI et doivent s'orienter vers des cabinets de conseil qui jouent le rôle d'un DSI à temps partagé. Les entreprises sont amenées à gérer leur relation avec les cabinets de conseil, en plus de leur relation avec un ou plusieurs fournisseurs cloud. Elles deviennent, dans la plupart du temps, dépendantes de ces acteurs. . Autre risque, qui résulte de cette dépendance, est celui de l'interopérabilité ou de la réversibilité des données, à savoir la capacité à changer facilement de fournisseur de cloud.

Enfin, il faut signaler les risques législatifs : le plus connu est la différence de protection des données entre la législation américaine (Patriot Act/Cloud Act) et européenne (RGPD).

Quelles sont les principales pratiques à mettre en place pour maîtriser le risque ? Quel rôle peut jouer le cloud souverain dans ces solutions ?

Le recours au cloud s'impose comme une obligation opérationnelle dictée par le marché. Aujourd'hui, utiliser une boîte email, c'est déjà bien souvent être utilisateur du cloud. Il est donc nécessaire pour les entreprises d'entamer une réflexion sur leur usage du cloud.

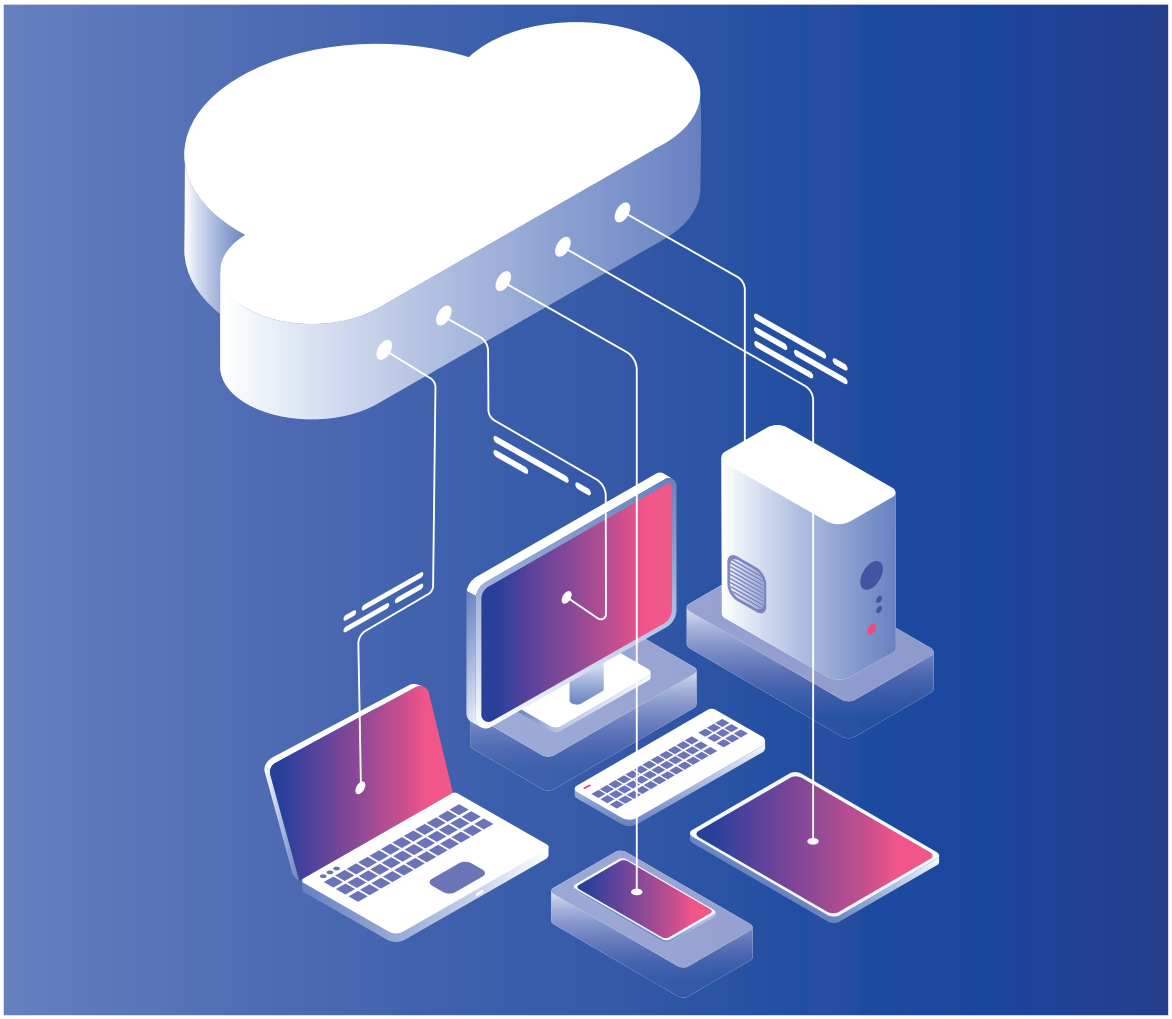
Le premier réflexe est de lister les types de données à héberger et de faire la distinction entre celles que l'entreprise souhaite continuer à héberger en interne et celles qui seront externalisées. La plupart des entreprises font le choix d'externaliser les données les moins sensibles et les moins spécifiques, à savoir, les données RH ou marketing. Par contre, elles auront tendance à conserver le stockage de données plus sensibles, comme les informations financières. La décision d'externaliser des données, et lesquelles, doit bien sûr prendre en compte le type de cloud – public, privé ou hybride – ainsi que la solution utilisée (open source ou propriétaire). Un cloud privé offre par exemple un meilleur niveau de sécurité qu'un cloud public. La relation de confiance qui s'installe avec le fournisseur de cloud est fondamentale dans cette réflexion – d'où l'importance des termes du contrat sur des points comme la réversibilité, l'existence et la fréquence d'audits de sécurité, etc. Le cloud souverain permet de minimiser les risques d'accès aux données par des tiers. Dans tous les cas, pour les données les plus sensibles, il est important de faire appel à un prestataire de cloud dont les données sont physiquement situées dans l'espace de l'UE pour bénéficier de la protection du RGPD.

La solution : le cloud de confiance

Le choix des solutions de sécurité proposées par les prestataires de Cloud est un enjeu stratégique pour toute entreprise ou administration. Le cloud de confiance implique notamment les mesures de sécurité suivantes :

- un contrôle et une gestion des identités renforcés ;
- un chiffrement des données stockées (le fournisseur de solutions cloud n'a ainsi aucun accès à vos données) ;
- une détection proactive des incidents de sécurité (anticipation et correction en temps réel d'une attaque) ;
- des pratiques de « Privacy by design » intégrées nativement ;
- un cloisonnement des traitements de données des clients.

Les mesures de sécurité physique supposent quant à elles le contrôle et la surveillance de l'accès physique aux centres de données, des contrôles environnementaux, la mise en place d'alimentations de secours, et l'existence de procédures de sécurité adaptées.



DES SOLUTIONS FLEXIBLES : CLOUD PUBLIC, PRIVÉ, HYBRIDE

De façon générale, **le cloud public** est basé sur une structure informatique qui n'appartient pas à l'utilisateur final (exemples : Alibaba Cloud, Microsoft Azure, Google Cloud, Amazon Web Services, IBM Cloud). C'est une solution dans laquelle plusieurs clients utilisent une même infrastructure partagée. Le cloud public n'a pas vocation à héberger vos données sensibles ou stratégiques, qui nécessitent un haut niveau de sécurité.

Le cloud privé est dédié à un seul utilisateur final ou groupe via des ressources informatiques stockées sur place ou dans le centre de données d'un fournisseur. Cette solution permet d'obtenir un niveau sécurité accru afin de protéger vos données sensibles et de se conformer à des réglementations strictes.

Le cloud hybride est composé de deux infrastructures cloud distinctes ou plus, pouvant être privées ou publiques, et qui restent des entités uniques mais sont connectées par une technologie standard ou propriétaire permettant la portabilité des données et des applications[10].
Les principaux avantages de ce modèle sont la flexibilité et la réactivité.

GREEN CLOUD

Le green cloud computing répond à la nécessité de réduire la consommation énergétique des data centers et leurs émissions de CO2, ou plus largement, leur empreinte environnementale ; sont donc également inclus la réduction des déchets, les types de matériaux utilisés (technique du refroidissement à eau ou à glace en add-on, notamment), et les économies de toutes autres ressources. Ceci permet aussi aux utilisateurs de profiter d'une meilleure gestion des coûts. En proposant des solutions « propres » qui répondent aux grands enjeux contemporains du cloud, le green cloud fait ainsi écho au cloud de confiance, voué à satisfaire de hautes exigences en matière de cybersécurité. Dans ce contexte, le green cloud a tout pour être partie prenante du cloud de confiance.

[10] Selon le National Institute of Standards and Technology (NIST)

Le cloud de confiance, une réponse à l'augmentation exponentielle du nombre de données sensibles

Des milliards de données sont générées dans le monde par les entreprises et l'administration. La constante digitalisation des usages, des démarches, ou encore la généralisation du travail à distance, ne font qu'ajouter à cette multiplication de données déjà exponentielle. Pour une grande part, ces données consistent en des informations relatives à des personnes physiques susceptibles d'être identifiées, directement ou indirectement : ce sont les données à caractère personnel.

Les traitements de ces dernières sont soumis à une réglementation stricte, le RGPD, sur le territoire de l'Union européenne. **Les données dites « sensibles »** constituent une catégorie particulière de données à caractère personnel et doivent en conséquence bénéficier de mesures de sécurité renforcées. Il s'agit par exemple des données de santé, de données reflétant les opinions politiques, religieuses d'une personne, ou encore de données biométriques.

L'atteinte aux données sensibles représente 10,4 % des violations de données à caractère personnel[11], exposant ainsi les entreprises et organismes publics à de lourdes sanctions financières en cas de manquement au RGPD. Les entreprises effectuant des traitements de données de santé sont ainsi particulièrement concernées par les problématiques d'hébergement hautement sécurisé.

<u>À noter</u> :
L'industrie pharmaceutique, les assureurs, les prestataires de santé font naturellement partie des acteurs privés appelés à protéger leurs données critiques au sein d'un cloud de confiance.

[11] Selon le baromètre FIC 2020 : https://www.forum-fic.com/Data/DO/tgBloc/23625/fr/params/file/data-breach-long.pdf

Du côté du secteur public, avec la modernisation des espaces de travail des administrations et l'accroissement des e-services publics, il est également nécessaire de limiter les risques en optant pour des solutions de cloud computing présentant les plus hauts standards de sécurité.

Autre terrain propice aux fuites ou manipulations de données : **la smart city et ses infrastructures connectées** (transports intelligents, bâtiments connectés, reconnaissance faciale, vocale etc.). La ville du futur hébergera en son sein des milliards de données, dont les données sensibles des « smart citizens » nécessitant une sécurité renforcée.

Les données de santé : des enjeux de sécurité au plus haut niveau

Quels types de données gérez-vous et comment sont-elles protégées ?

Au-delà des données « classiques » de toute entreprise, nous gérons des données spécifiques liées à l'activité de l'Institut Pasteur de Lille. À savoir des données de recherche qui peuvent inclure des données à caractère personnel anonymisées. Nous traitons également des données liées à nos activités de santé : ils peut s'agir par exemple de données à caractère personnel dans le cadre d'actes de prévention ou de données rattachées à nos essais cliniques. Nos différentes activités nous amènent enfin à gérer des données dites sensibles.

Pour protéger les plus sensibles de ces données, nous avons mis en place un niveau élevé de sécurité informatique répondant aux exigences de l'ANSSI.

Quels sont les principaux risques pesant sur ces données, en particulier dans le contexte actuel de Covid-19 ?

Les cyberattaques peuvent concerner toutes les catégories de données que nous traitons, des données de santé à celles du personnel lié à l'Institut en passant par les données de recherche.

Dans notre secteur, le risque d'espionnage industriel est une réalité bien concrète. L'émergence de la Covid-19 a logiquement accentué les cybermenaces envers les données ayant trait à des virus ou à différents pathogènes. Les différents organismes et pays se livrent à une véritable course au vaccin, et dans ce contexte, ces données sont encore plus précieuses.

Envisagez-vous l'hébergement de vos données auprès d'un Tiers de confiance ?

Externaliser les données sensibles chez un prestataire agréé hébergeur de données de santé permet de garantir un niveau de sécurité optimum des données puisque ces hébergeurs doivent se conformer à des exigences importantes en matière de cybersécurité. De nombreuses organisations font aussi ce choix parce qu'il permet un partage de la responsabilité juridique en cas de cyberattaques.

Néanmoins, pour un cloud de confiance permettant d'échapper au Cloud Act, il est nécessaire de choisir un prestataire français – ou au minimun européen – sans aucun lien, même capitalistique, avec une entreprise de droit américain.

À noter : Le stockage des données en dehors de l'UE et sur le Privacy Shield

Le RGPD n'exige pas un stockage des données à caractère personnel au sein de l'UE : il autorise le transfert de telles données dans un pays tiers, si ce dernier assure un niveau de protection adéquat. Depuis le 16 juillet 2020[12], le recours au Privacy Shield a été déclaré invalide par la Commission européenne. Cette série de dispositions, mise en place depuis 2015-2016, réglementait jusque-là les transferts des données personnelles depuis l'UE vers les États-Unis. Elle précisait les règles de protection de ces données que s'engageaient à suivre les entreprises américaines pour être considérées comme certifiées. Cette certification leur permettait de transférer légalement des données personnelles protégées par le RGPD vers les États-Unis.

En juillet 2020, la Commission a jugé que le Privacy Shield ne respectait pas suffisamment les exigences du RGPD en matière de protection des données personnelles provenant de l'UE. La fin du Privacy Shield ne signifie cependant pas l'interdiction du transfert de données vers les États-Unis. Les entreprises concernées doivent désormais signer des clauses contractuelles attestant que les conditions de transfert sont conformes aux exigences du RGPD.

À noter : Si les organismes privés et publics doivent veiller à la protection de leurs données stratégiques afin de ne pas mettre en péril leur fonctionnement, le RGPD les oblige par ailleurs à sécuriser les données qu'ils recueillent et utilisent.

Ceci implique notamment le recensement des activités de traitement de données personnelles réalisées, l'indication des catégories de données personnelles traitées, mettant en lumière les données sensibles, et la destination et l'origine des flux de données, mettant en évidence les transferts de données hors Union européenne.

La solution : un Cloud de confiance mis en place par un Tiers de Confiance

L'offre cloud fournie par un Tiers de Confiance permet aux utilisateurs de bénéficier d'une chaîne de services de confiance numérique garantissant sécurité des données à caractère personnel et respect des réglementations. Cette solution repose notamment sur des fonctionnalités « Crypto as a Service », telles que la signature avancée et qualifiée, l'horodatage qualifié, la Public Key Infrastructure ou encore les « Hardware Security Modules ». Ces boîtiers HSM offrent des fonctions cryptographiques et sont considérés comme inviolables.

[12] Selon un arrêt de la Cour de Justice de l'Union européenne

Le cloud & les datas, un enjeu pour les États

Malgré l'échec des premières tentatives françaises de cloud souverain, la France reste consciente de la nécessité de protéger ses données sensibles, celles des collectivités et des secteurs d'activité d'importance stratégique. Le récent projet de développement d'un cloud de confiance a dorénavant vocation à sécuriser les données de toutes les entreprises, et en particulier celles du secteur industriel, les craintes d'espionnage pesant fortement dans la balance. Au niveau européen, les initiatives réglementaires se multiplient pour définir un cadre de cybersécurité de plus en plus précis, s'adressant à la fois aux secteurs privé et public.

Le Cloud Act, une menace sur la sécurité de vos données ?

En matière de sécurité du cloud computing, une des plus grandes préoccupations des États européens et de l'Union européenne réside dans l'adoption par les États-Unis du Cloud Act (« Clarifying Lawful Overseas Use of Data Act »). Cette loi fédérale de 2018 permet aux agences de surveillance américaines d'accéder aux données stockées par des prestataires de cloud américains, que leurs data centers se situent sur le sol des États-Unis ou à l'étranger. Si cette loi a pour vocation la lutte antiterroriste, elle constitue pour les États de l'UE et leurs entreprises une brèche considérable en matière de cybersécurité ainsi qu'une porte ouverte à l'espionnage économique. Le Cloud Act représente aussi une porte d'entrée pour la pratique du LOVEINT (love interest), grâce à laquelle les employés des agences de surveillance utilisent leurs prérogatives à des fins personnelles.

Pour la Cour de Justice de l'Union européenne (CJUE), l'extraterritorialité de la loi américaine et les pouvoirs étendus des autorités américaines en matière de surveillance et de sécurité publique excèdent « le strict nécessaire »[13]. La localisation des data centers sur le sol français ou européen n'est donc pas une garantie de sécurité suffisante lorsque l'on fait appel à un prestataire de cloud étranger.

[13] CJCE, arrêt du 16 juillet 2020 invalidant le « Privacy Shield »

En réponse au Cloud Act, l'UE travaille actuellement sur un projet de règlement relatif à l'accès transfrontalier aux preuves numériques, l'objectif étant de faciliter la communication des preuves électroniques stockées dans le nuage en vue de les utiliser dans le cadre de procédures pénales.

La mise en place du RGPD, une incitation à la sécurisation des données au niveau européen

Depuis 2018, respecter le RGPD constitue un enjeu stratégique pour les entreprises, et donc pour les prestataires de cloud, afin de se prémunir de l'application de lourdes sanctions pécuniaires en cas d'infraction aux exigences imposées par le règlement.

Dans un second temps, la conformité au RGPD est devenu un facteur rassurant pour les clients, qui voient dans cet engagement des fournisseurs de solutions cloud un gage de sécurité et de confidentialité. Ainsi, un prestataire déclaré conforme au RGPD, et dont lesdatacentersetéquipessontsitués en France ou en Europe, devient progressivement synonyme d'une véritable protection des données.

Si le RGPD agit désormais comme un « label » pour les entreprises et leurs prestataires, sa bonne application n'est pas moins capitale pour l'administration nationale ou les institutions européennes. Il revient par ailleurs au Contrôleur européen de la protection des données (CEPD), autorité de contrôle indépendante, de veiller à l'exemplarité des organes de l'UE en cette matière.

L'État français protège ses données. Au-delà des tentatives de création de cloud souverains, l'État français s'est également montré particulièrement sensible à la sécurité des données de ses administrations et collectivités, en interdisant par exemple la localisation des archives publiques en dehors du territoire national. Avec l'entrée en vigueur du règlement européen relatif au libre flux des données à caractère non personnel[14], il appartiendra à l'Etat de modifier sa législation en autorisant le stockage des données des archives de documents courants au sein de l'Union européenne, et ce avant le 30 mai 2021. Les archives « historiques » et celles relevant de la sécurité publique ne feront toutefois pas partie de cet assouplissement.

[14] RÈGLEMENT (UE) 2018/1807 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 14 novembre 2018 établissant un cadre applicable au libre flux des données

Labéliser et sécuriser la confiance

Outre la réglementation, la sécurisation de la data dans l'univers de l'informatique en nuage comprend de nombreuses normes, labels ou certifications. De portée internationale, la certification ISO27001 assure par exemple un niveau de sécurité optimal des données, applications, plateformes et infrastructures, et inclut la mise en place de dispositifs d'audit, de surveillance et de mesure d'un Système de Management de la Sécurité de l'Information (SMSI). Délivré par l'Agence nationale de sécurité des systèmes d'information (ANSSI), le label SecNumCloud représente quant à lui le graal de la qualification des opérateurs de cloud computing, faisant d'eux des prestataires de confiance. Ce label s'adresse en premier lieu à des organismes soumis à une réglementation stricte, tels les Opérateurs d'Importance Vitale (OIV) ou certaines administrations, et manipulant des données hautement confidentielles.

La certification Hébergement des données de santé (HDS) est quant à elle destinée à « toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même[15].»

[15] L.1111-8 du code de la santé publique, modifié par la loi n° 2016-41 du 26 janvier 2016

Les hébergeurs de ces catégories de données doivent être certifiés par un organisme accrédité, et donc répondre à des conditions précises en matière de sécurisation de ces données particulièrement sensibles.

Des initiatives à l'échelon européen

Si l'État français promeut ardemment la création d'un cloud de confiance 100 % français, cela ne l'empêche pas d'être partie prenante d'initiatives du même ordre au niveau européen. Le projet Gaia-X, collaboration entre la France et l'Allemagne, a ainsi pour vocation l'émergence d'une infrastructure européenne de données « s'appuyant sur les principes d'ouverture, d'interopérabilité, de transparence et de confiance[16] ».
Concrètement, il s'agit pour les deux pays de parrainer un catalogue de services numériques conformes à des standards préétablis et offrant un haut niveau de sécurité. Cette action coordonnée témoigne de la volonté des acteurs européens d'ériger un rempart contre l'application de lois extra-territoriales, tout en offrant une alternative innovante aux solutions proposées par les GAFAM.

La solution : le cloud français

Pour de nombreuses raisons, le cloud français offre transparence et haut niveau de garanties quant à la sécurité de vos données :

- stockage des données en France
- contrats commerciaux de droit français
- respect des réglementations protectrices européennes (RGPD, notamment)
- certifications ISO 27001, HDS…
- absence de risque d'extra-territorialité des réglementations des pays tiers.

[16] Bruno Le Maire, ministre de l'Économie et des Finances, Communiqué de presse conjoint du 4 juin 2020

Conclusion

Les initiatives récentes de développement d'un cloud de confiance mettent clairement en évidence les atouts des acteurs français et européens pour une innovation numérique transparente et sécurisée, synonyme de nombreux avantages pour les responsables de traitements de données.

Ces différents projets sont également empreints d'une volonté forte de l'Europe et de ses pays membres d'acquérir une indépendance technique et économique dans le secteur de la donnée numérique et du cloud computing.

En tout état de cause, cette indépendance numérique passe nécessairement par la capacité de se prémunir de l'ingérence juridique ou judiciaire de pays tiers. Confier l'hébergement de vos données aux GAFAM ne vous garantit en rien leur totale sécurité : le Cloud Act permet en effet aux instances judiciaires américaines de contraindre ces prestataires à leur fournir vos données, dans le cadre d'un mandat ou d'une assignation.

À l'inverse, en recourant aux services d'un prestataire français, hébergeant vos données en France et auprès d'un hébergeur n'ayant aucun lien, (ne serait-ce que capitalistique), avec une entreprise de droit américain, vous vous assurez leur entière sécurité et la seule application des lois de la République. Vous offrez ainsi à vos données, et en particulier les plus sensibles, un niveau de sécurité à la hauteur des attentes des usagers mais aussi des normes en vigueur en France et en Europe.

L'offre de cloud de confiance Certigna

Qui mieux qu'un Tiers de Confiance français pour sécuriser, héberger, stocker, et archiver vos données en toute transparence ?
Certigna, filiale cybersécurité du groupe Tessi, propose une offre d'hébergement et d'infogérance : CERTIGNA CLOUD.

Faire appel à Certigna Cloud du groupe Tessi, c'est s'assurer :

- du stockage des données en France
- du respect des réglementations européennes et des normes internationales
- de l'emploi de très hauts niveaux de sécurité et du chiffrement des données
- de l'utilisation de solutions green permettant de gérer au mieux l'empreinte carbone du cloud.

En tant que Tiers de Confiance, **Certigna vous fait également bénéficier d'un ensemble de fonctionnalités « Crypto as a Service »** (signature avancée et qualifiée, horodatage qualifié, Public Key Infrastructure, etc.), ainsi que de l'hébergement et de la gestion de vos propres outils crypto (type HSM).

Déléguez la gestion de vos supports et services cryptographiques à des experts de la confiance numérique en faisant appel à Certigna.

CERTIGNA by tessi